How to keep the world's eyes out of your webcam

November 21 2014, by Michael Cowling

It’s the standalone webcams that are at risk. Credit: Flickr/mrmayo, CC BY-NC

There are concerns that thousands of private webcams around the world could be streaming live images to anybody who wishes to view them – without their owner knowing – thanks to a Russian website providing a convenient list of every camera that can be accessed.

But how is the website doing this? Just like with those who had concerns over Facebook's Messenger app, the website is exploiting the fact that most users accept the default settings on webcams. People integrate technology into their lives without any thought about the security or privacy settings, blindly pressing "yes" when faced with a piece of technology asking you to stop and consider.

Peering into people's lives

The issue has arisen over the past few years as webcams have grown to include extra features in a bid for customers' business.

One of these features is the ability to access an external webcam over the internet from anywhere in the world from your smartphone, tablet, laptop or any web browser enabled device.

To allow this, the webcam connects to a user's local home network and obtains an internet protocol (IP) address from their router. This then allows users to dial back into the webcam using that address and view the video field. This is useful for those using cameras for home/business security purposes, home support services or even just to check on the whereabouts of the family cat!

In the battle for new customers, many manufacturers have started to add features like these to separate their technology from the pack.

Unfortunately, the problem arises when the cameras are manufactured in the factory and the software is loaded. To make this process easier, each camera is given the same default username and password to use as a log in when accessing remotely.

While users are encouraged to change their password, some don't. So the camera is made available to the world via the internet with a default

password that is easily known to anyone who has bought the same type of camera (or can read it on the manufacturer's website).

It is then a simple matter for unscrupulous types to scan for these cameras over the internet (by looking for devices using the correct ports) and then use the default password to log in and view the feed, keeping track of the details of each camera for collation on a website.

Cameras on baby monitors, closed-circuit TV monitoring as well as standalone webcams are all at risk from being access by the Russian website.

Webcam concerns

The issue was first revealed in September but has now raised concern around the world with the UK's information commissioner urging Russian authorities to take down the website.

The Australian government also raised the alarm this month over the then .com website. There are now reports that the website's new .cc domain name is registered to the Australia-administered Cocos Islands.

The majority of media reports so far have decided not to give the actual web address for the site but despite the global concerns it is still active, and registered via a popular domain name company.

The actual website lists more than 17,000 webcams in 126 countries, including 284 in Australia. The Australian camera images show the inside of shops, offices and homes, outside in gardens, doorways and driveways and a few baby cots and child play areas.

The website says the cameras are not hacked and access is only possible because they were left on "default password".

What can we do?

So, how can people protect against this problem? First, it's important to note that the issue only affects cameras that can be accessed remotely over the web. This means that, unless you've installed special software, your camera in your smartphone, tablet or laptop is safe from this type of exploit.

But if people do have a standalone camera (that either attaches to your computer in some way or is freestanding), then they should check their user manual and packaging for the camera to see if it claims to be accessible over the internet remotely.

If it does, then users should immediately change the password to access the camera over the internet. Instructions on how to do this should be available via the manual for the product or the manufacturer's website. It's as simple as that.

Isn't this illegal?

Unfortunately, the methods by which people are accessing these cameras, while being unethical, are not actually illegal.

These cameras have been built to be accessed over the internet and individuals are using freely available tools and information to find and access these cameras.

While it might be the case that the Russian website eventually gets taken down due to government and media pressure, the exploit will continue to exist and webcams will continue to be available and images viewed until users close the gap by changing their passwords to something other than the default.

Privacy vs convenience of technology

The bigger question though is how did this happen? While a finger could be pointed at the manufacturer for using the same password for every device, responsibility also needs to rest with the user to make sure that they are not allowing their own inability to follow password guidelines and read security messages to interfere with their need for privacy.

As with the Facebook Messenger issue, the broader issue here comes back to our willingness to allow important decisions about our privacy to be quickly skimmed over with the hurried press of an "agree" button or the use of webcam without a glance at the instructions.

Until we can reconcile our use of technology with our desire for privacy and ensure that we all understand what we are using, these problems will continue to occur.

Perhaps this will ultimately take legislative intervention, requiring the government to save us from our own ambivalence.

This story is published courtesy of The Conversation *(under Creative Commons-Attribution/No derivatives).*

Source: The Conversation

Citation: How to keep the world's eyes out of your webcam (2014, November 21) retrieved 23 April 2024 from https://phys.org/news/2014-11-world-eyes-webcam.html