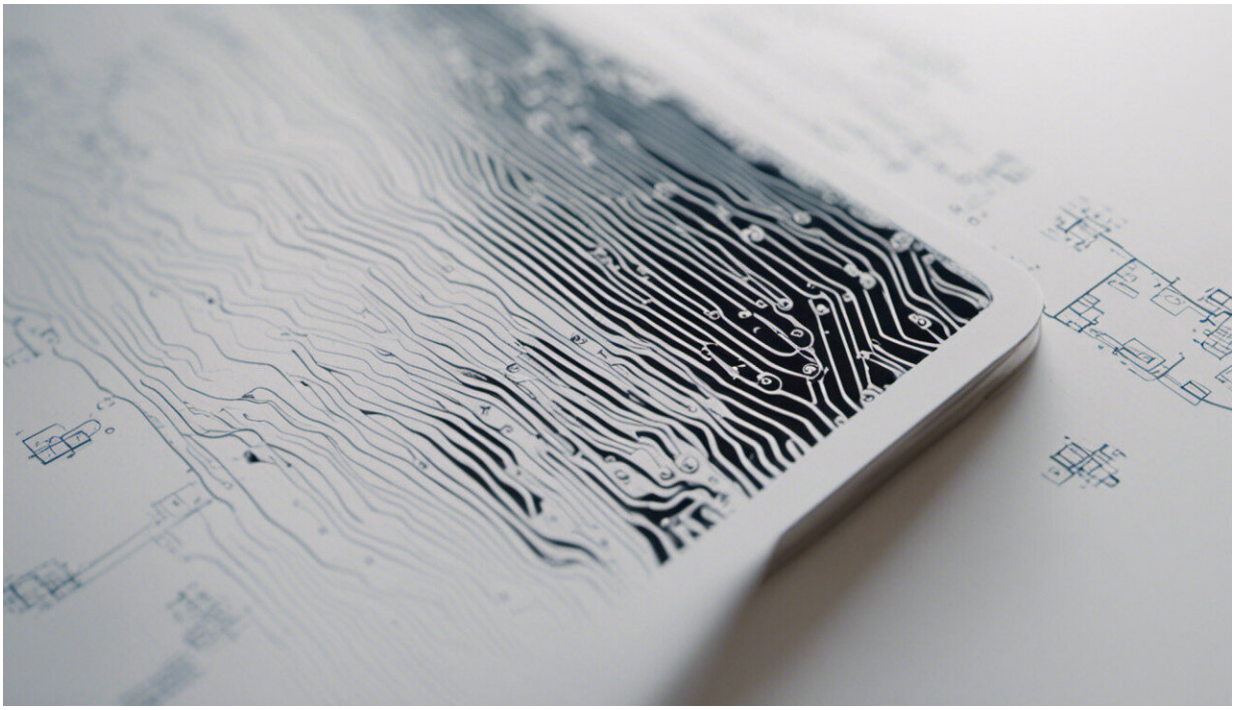
Hackers can access your mobile and laptop cameras and record you: Cover them up now

April 16 2020, by David Cook



Credit: AI-generated image (disclaimer)

Whether you use Zoom, Skype or Microsoft Teams, the webcam on your home PC or laptop device has probably never been as active as it is during this pandemic.

Most of us have a camera built into our phone, tablet, laptop, or a

desktop webcam we use for work, study or virtual socializing.

Unfortunately, this privilege can leave us vulnerable to an online attack known as camfecting. This is when hackers take control of your webcam remotely. They do this by disabling the "on" light which usually indicates the camera is active—so victims are none the wiser.

Many of our device cameras remain unsecured. In fact, research has suggested globally there are more than 15,000 web camera devices (including in homes and businesses) readily accessible to hackers, without even needing to be hacked.

Take a tip from Mark Zuckerberg

When your laptop is turned off its webcam can't be activated. However, many of us keep our laptops in hibernation or sleep mode (which are different). In this case, the device can be woken by a cybercriminal, and the camera turned on. Even Mark Zuckerberg has admitted he covers his webcam and masks his microphone.

The number of recorded instances of image captured through unauthorised webcam access is relatively low. This is because most attacks happen without the user ever realizing they've been compromised. Thus, these attacks go unaccounted for.

It's important to consider why someone would choose to hack into your home device. It's unlikely an attacker will capture images of you for personal blackmail, or their own creepy exploits. While these instances do eventuate, the majority of illicit webcam access is related to gathering information for financial gain.

Say cheese!

Cybercriminals frequently attempt tricking people into believing they've been caught by a webcam hack. Everyday there are thousands of spam emails sent in a bid to convince users they've been "caught" on camera. But why?

Shaming people for "inappropriate" webcam use in this way is a scam, one which generates considerable ransom success. Many victims pay up in fear of being publicly exposed.

Most genuine webcam hacks are targeted attacks to gather restricted information. They often involve tech-savvy corporate groups carrying out intelligence gathering and covert image capturing. Some hacks are acts of corporate espionage, while others are the business of government intelligence agencies.

There are two common acquisition techniques used in camfecting attacks. The first is known as an RAT (Remote Administration Tool) and the second takes place through false "remote tech support" offered by malicious people.

Genuine remote tech support usually comes from your retail service provider (such as Telstra or Optus). We trust our authorized tech support people, but you shouldn't extend that trust to a "friend" you hardly know offering to use their own remote support software to "help you" with a problem.

An example of an RAT is a Trojan virus delivered through email. This gives hackers internal control of a device.

Total access

When a Trojan virus infects a device, it's not just the webcam that is remotely accessed, it's the whole computer. This means access to files,

photos, banking and a range of data.

The ability to install a RAT has been around for several years. In 2015, a popular RAT could be purchased on the internet for just US $40. The malware (harmful software) can be deployed via an email, attachment, or flash drive.

Those wanting to learn how to use such tools need look no further than YouTube, which has many tutorials. It has never been easier for hackers.

Webcams are everywhere

Our homes are getting "smarter" each year. In 2018, the average Australian household reportedly had 17 connected devices.

Let's say there's one or two laptops, three or four mobile phones and tablets, a home security camera system and a smart TV with a built-in camera for facial recognition.

Add a remote video doorbell, a talking doll named My Friend Cayla, the drone helicopter you got for Christmas, and the robot toy that follows you around the house—and it's possible your household has more than 20 IP accessible cameras.

To better understand your vulnerabilities you can try a product like Shodan. This search engine allows you to identify which of your devices can be seen by others through an internet connection.

Practise 'cyberhygiene' at home

Placing a piece of black tape over a camera is one simple low-tech solution for webcam hacking. Turning your laptop or desktop computer

off when not in use is also a good idea. Don't let a device's hibernation, sleep or low power mode lure you into a false sense of safety.

At work you may have firewalls, antivirus, and intrusion detection systems provided by your company. Such protections are void for most of us when working from home. "Cyberhygiene" practices will help secure you from potential attacks.

Always use secure passwords, and avoid recycling old ones with added numbers such as "Richmond2019," or "Manutd2020". Also, make sure your antivirus and operating system software is regularly updated.

Most of all, use common sense. Don't share your password (including your home wifi password), don't click suspicious links, and routinely clear your devices of unnecessary apps.

When it comes to using webcams, you may wonder if you're ever completely safe. This is hard to know—but rest assured there are steps you can take to give yourself a better chance.

Provided by The Conversation