At National Online Safety we believe in empowering parents, carers and educators with the information they need to hold an informed conversation about online safety with their children, should they feel it is needed. Please visit nationalonlinesafety.com for further guides, ghints and tips for adults.

Part of our Privacy & Security Series

NOS Online Privacy & Security

Brought to you by National Online Safety®

www.nationalonlinesafety.com

What you need to know about... WEBCAMS



What are they?

'Webcams'

Most commonly found embedded in laptop screens and smartphones, webcams are tiny video/still cameras designed to let you participate in video calls on services such as Skype and Zoom. They have become hugely popular since the start of the coronavirus pandemic, allowing homeworkers to chat with remote colleagues and helping friends and families stay in touch. However, there are many security and privacy risks associated with webcams that owners should be aware of.



Know the Risks

Hackers

Webcams are a prime target for hackers as they give attackers a highly intrusive eye into the victim's home. There have been several high-profile breaches where integrated laptop webcams or dedicated webcams have been targeted.

Malware

Malware often targets webcams, secretly giving hackers access to your computer's webcam without any visible signs that the camera is switched on. Such malware can arrive in email attachments or by clicking on rogue links on websites, and it can often install itself in the background without the user being alerted.

Access to strangers

Children can be naïve to the dangers of allowing strangers to access the computer's webcam. They may click through warning messages that grant access to the camera or they may willingly share the camera with people they meet online who are pretending to be children.

Blackmail

Webcams can be used for blackmail, even when the webcam itself hasn't been hacked. Fraudsters will claim to have webcam footage or stills of the victim whilst naked or accessing pornography and threaten to post such footage on social media or send it to employers if the victim fails to pay up. The fraudsters normally don't have any footage at all, but the threat is often enough.

Look out for...

The indicator light

It can be difficult to tell if your webcam has been compromised or is secretly capturing footage. If the little indicator light (normally green) next to the webcam is lit when you don't expect it to be, this could be a sign.

Camera permissions

Check the camera permissions on your computer to ensure no rogue or unnecessary apps have been granted access to the camera. Switch off any apps that don't need access to the camera. If you never use the webcam, you can bar all access to the webcam. Better still, cover it when not in use.

Unexpected saved folders

Another telltale sign of a webcam compromise is folders containing videos or photos taken by your webcam appearing on your computer. Malware will often save videos/photos on your machine before attempting to upload them to the hackers, who will then use them for blackmail purposes. Check your Photos and Videos folders occasionally for any unexpected files.



User Safety Tips

Explain the dangers to children

Talk to your children about the dangers of talking with strangers via webcam and tell them not to accept any video chat requests from people they don't know in real life. Keep computers in family rooms, so that children can't covertly use the webcam in their bedrooms.

Refuse & report

Do not pay anyone claiming to have captured embarrassing webcam footage of you. It's highly likely they don't have footage in the first place, and even if they do, paying them may encourage them to demand more money. Report the matter to the police and keep a record of any evidence you can.

Unplug webcams & update firewalls

Unplug external (USB) webcams when they're not in use. Make sure your computer is running up-to-date security software and that the firewall is switched on. This can thwart attempts to access your webcam remotely.

Our Expert

Barry Collins



Barry Collins has been a technology journalist and editor for more than 20 years, working for titles such as The Sunday Times, Which?, PC Pro and Computeractive. He's appeared regularly as a technology pundit on television and radio, including on BBC Newsnight, Radio 5 Live and the ITV News at Ten. He has two children and has written regularly about internet safety issues over the years.

Users of this guide do so at their own discretion. No liability is entered into. Current as of the date of release: 05.08.2020