Cyber Spies: How to Safely Use Webcams and Video Conferencing

Follow these six tips to help you select a safe video conferencing platform and secure your webcam:

"Free" is not usually free

Free services may not invest as much in security. Do your research and consider choosing a paid web conferencing solution if their security measures are more robust. Instead of using unsecure free Wi-Fi hotspots, create your own personal hotspot with your corporate mobile device.

Look around your office

How much personal or proprietary information could be exposed by the items in your space? A video conferencing platform with a virtual background or greenscreen can help conceal your personal environment and any confidential information that shouldn't be shared.

Secure your webcam

Turn off the external webcam and only connect when needed to prevent cyber spying. For an internal webcam, such as in a laptop, you can affix a Post-It note over the camera lens.

Restrict meeting access

Choose a platform that makes it difficult to conceal or change your identity information and ask all attendees to announce themselves at the start of the meeting.

Insist on end-to-end encryption

It provides an extra layer of security that makes conferences and communication harder to intercept.

Install security software

Ensure the antivirus and anti-spyware software on your computer is up to date. Setting up a firewall or configuring your internet router to block unwanted incoming internet traffic can add another level of protection for your webcam, computers, and other devices on your home network. Ensure your wireless network has strong security settings and a strong password to prevent external parties from accessing your Wi-Fi network without your consent.

ANCHOR
RISKsolutions Corp.

Source: CyberScout