Webcam spy. *Protect your privacy and use these tips to keep hackers from hijacking your webcam.*

Thanks to COVID-19, video conferencing is the new trend across organizations, including the Postal Service.

While this technology allows us to collaborate in new and exciting ways, you must take precautions to prevent hackers from hijacking your webcam and using it to snoop. This snooping could not only affect your personal life, but on meetings where they may learn about sensitive information that could compromise the organization.

While most of us are using laptops with installed webcams, follow these tips to help protect your privacy:

- **Cover it up.** Physically cover up your webcam with electrical or masking tape, or a webcam cover, when not participating in a work-related teleconference.

- **Turn it off.** Close your laptop or turn off your computer when not using it.

If you have an external camera you use at home, it is important to use these additional tips:

- **Unplug it.** Turn off your device and unplug it when not in use. Like personal home assistants, webcams could spy on you without your knowledge.

- **Change your password.** If your webcam came with a default password — often known to hackers — reset it.

- **Keep software up to date.** Stay current on all software updates and security patches to close any doors hackers might try to enter.

- **Use trusted tech support.** Unethical technicians and remote support help could leave your webcam vulnerable to hijacking if they were to install remote-access programs. Make sure you trust those working on your hardware.

***