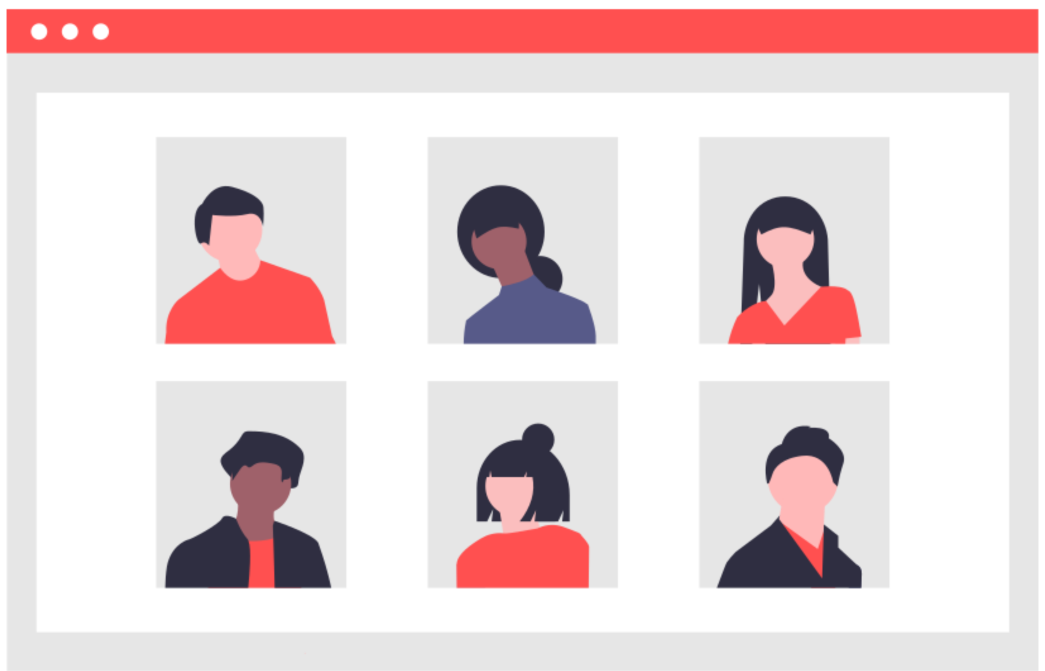
Staying Secure and Private in Zoom



Zoom has quickly become the de facto standard for online business meetings. With the rapid rise in adoption, an equally rapid rise in attention from security researchers and privacy advocates has surfaced a range of concerns for those hosting and participating in Zoom meetings.

It's exceptionally easy for people to connect online using Zoom, a fundamental need we're all facing as we lock ourselves away at home. To make connections super easy, Zoom's default configuration goes without a number of security and privacy controls.

Watch out for

🤫 Sensitive discussions

☠️ Dodgy software

😈 Bad behaviour

🙊 Privacy disclosure

THE GOOD NEWS Simple measures can help you stay secure and private in Zoom meetings.

Before joining meetings

□ Make sure emails appearing to come from Zoom are legitimate.
□ If possible join using the browser version only.
□ If you need to install the software, make sure you're installing it from a trusted source: https://zoom.us/download
□ Regularly check for software updates to make sure the latest security bugs are fixed.
□ Familiarise yourself with any meeting ground rules.
□ Find a private location for meetings if confidential information is being discussed.

During meetings

□ Limit the personal information you share when entering or during a meeting.
□ Take care when clicking on links or attachments shared during the meeting.
□ If you're not participating in the meeting, disable your camera and microphone.
□ Consider using a webcam shield or tape over your camera if you don't need it.
□ Carefully check what's visible before sharing your screen.
□ Be mindful that the meeting host can tell if you click away from the meeting window.
□ Flag any inappropriate behaviour with the meeting host or moderator.

After meetings

□ Contact the host if you have any concerns about your privacy or security.
□ Uninstall Zoom software from your device if you no longer need it.