How to Keep Your Zoom Chats Private and Secure

With so many people stuck inside, Zoom has become the default video chat platform for millions. Its simple, accessible interface makes keeping in touch with family, friends, and coworkers a cinch. At the same time, many have found Zoom's default privacy and security features lacking, exposing users to trolls and unwanted oversight. If you're using Zoom, here's how to stay safe and protected.
First keep in mind that Zoom's security is fine for most people. If your meetings are more sensitive, though, you should know that the platform's claims of end-to-end encryption don't really hold up, and critics have found the type of encryption it does implement lacking in some ways. There are some suggestions for other platforms that have more robust encryption in place below.

For privacy and trolling concerns, though, there are plenty of settings you can tweak to make Zoom a safer place for you and everyone else on the line.

Stop Zoombombs

Every Zoom meeting is based around a 9-digit meeting ID. If that ID becomes public somehow, or trolls find it in a web search or guess it, they can pop into your chats and disrupt them. That's obviously a problem, and an increasingly common occurrence.

You've got a few ways to guard against this. First and most obviously, be careful who you share the meeting ID with; posting it on your public Twitter feed isn't the best idea. Bear in mind that contacts you've added in Zoom will be able to see your Personal Meeting ID, and so will know how to find any meetings you launch with it.

When you launch or schedule a meeting, the options panel lets you generate a random ID for the meeting rather than using your personal one. Using a random ID is another way to avoid trolls, though if you've got an office team who always meet with the same ID, you might not consider the extra inconvenience worth it.

To absolutely lockdown a meeting, make sure participants need a password to access it. Again, this can be found in the options pane when you create or schedule a meeting. Of course, be careful how you share the password and who you share it with.

Finally, if you look under the advanced options for hosting meetings, you'll see an Enable Waiting Room option. People are put on hold here before you give them specific approval to join, and it can help to block out anyone you weren't expecting. All these options can be set on a meeting-by-meeting basis, or configured as defaults by going to your Zoom settings on the web.

Restrict Users

Even with those precautions in place, you're still not completely protected against unwanted guests, or indeed from bad behavior by the guests that you have invited to your video chat. As a host, you've got a few handy options for limiting what other users can do.

For starters, you can restrict screen sharing: If you go to your Zoom settings on the web and click **In Meeting (Basic)**, you'll see a **Screen sharing** option to stop anyone except you from sharing the desktops or apps on their computer. You can still grant screen sharing privileges to specific users in a meeting later, if you need to.

The same option is available after you've launched a meeting on Windows or macOS. Click the small arrow next to **Share Screen**, then **Advanced Sharing Options**, and you can ensure that only you can bring up videos, images, or anything else from your computer or phone.
Most Popular

Another step you can take is to lock a meeting once you're sure that everyone who needs to join has joined. From the desktop app, click **Manage Participants**, **More**, and then **Lock Meeting**. Just make doubly sure that you weren't expecting someone who hasn't yet arrived, as they won't be able to get in.

Add all of these measures up together and you can be very confident that your next Zoom meeting isn't about to get rudely interrupted. Be careful not to get complacent though, particularly when it comes to limiting the exposure of the meeting IDs and the passwords that you're using for your video calls.

Stay Private

So you're safe and protected from outsiders; all that's left is an awareness of what your boss can peek at while you're using Zoom as a meeting participant. Meeting hosts have a lot of privileges and tools at their disposal, which you should know about going in.

Zoom had an attention-tracking feature, for instance, that told hosts if participants clicked away from the Zoom app for more than 30 seconds. After a public backlash, Zoom deactivated the feature last week.

Also remember that hosts can record audio and video from meetings in full, as well as keep a record of public chats. What's more, if you save the chat log for yourself, it will also include private chats you've been involved in, so be very careful about sharing that file with anyone else. Don't just post it in the group chat for everyone to read. If a host chooses to enable this setting, Zoom will notify you and give you a chance to opt out.

There's not a lot you can do about these features, which are designed to make it easier to create logs for people to look back on later, but it's worth knowing about them. A simple rule of thumb: If there's a communication you don't want anyone else to know about, keep it off Zoom.

Try an Alternative

If you're not happy with Zoom, then you've got plenty of other options to turn to. For example, **Google Duo:** it recently updated the maximum video chat group size from 8 to 12, it's available on mobile devices and the web, and video and audio calls are end-to-end encrypted (not even Google can peek at the data).

For those of you with colleagues, family, and friends who are all on Apple devices, **FaceTime** is an option. Group video chats of up to 32 people are supported, end-to-end encryption is turned on by default, and the apps are simple to use across iOS, iPadOS, and macOS. The downside is, of course, that no one on Windows or Android can join in.

Webex from Cisco is another group video calling tool that supports end-to-end encryption: It's a little business-focused, but you do get support for video calls of up to 100 people, and a lot of the same features that Zoom brings to the table. The free tier is quite generous at the moment, though we'll have to wait and see if it remains so after the current global pandemic has passed.

Like Webex, **GoToMeeting** has been in the virtual meeting business a long time, and includes end-to-end encryption as standard. Unlike Webex, there are no free plans, so you or your company will have to pay $12 a month and up for video calls with up to 150 different people. There's also a 14-day free trial.

If you can live without full end-to-end encryption-so you're essentially putting your trust in the software developer not to gather any more data than it needs to-then programs such as **Skype** (up to 50 people on a video call), **Slack** (up to 15 people on a video call with a paid plan), and **Facebook Messenger** (up to 50 people on a video call) are all options as well.