# *How to Prevent Zoom-Bombing*

Zoom is becoming the videoconferencing method of choice during the COVID-19 pandemic. Unfortunately, your Zoom meetings are wide open to hijacking if you don't know how to set the host controls properly. Learn how to stop bad actors and keep your video calls on track. As with many security measures (digital and non-digital), they often provide an extra layer of inconvenience. It is up to each host to determine the risk of their meeting being hijacked and then implementing the necessary safeguard accordingly.

**1. Use a Unique ID for Large or Public Zoom Calls**

When you create a Zoom account, the app assigns you a Personal Meeting ID (PMI). It's a numeric code that you can give out to people when you want to meet with them. You can use it over and over; it doesn't expire. For standing meetings with a team or a weekly check-in, using the same code makes sense because people can join without having to hunt down this week's login number. It's always the same.

Zoom also gives you the option to *not* use your PMI for a meeting and instead generate a unique code. If you're the host of a large Zoom call where members of the public or other strangers are invited, it's much better to use a one-time code rather than your PMI. Here's why: Once you put  your PMI into the world, people can use it to try and jump in on your Zoom calls at any time.

When you schedule a Zoom meeting, look for the Meeting ID options and choose Generate Automatically. Doing so plugs up one of the biggest holes that Zoom-bombers can exploit.


**2. Require a Meeting Password**

Let's say you publicly invite people to join a meeting, but you require an RSVP and are vetting the list of respondents. One way to protect the meeting is to require a password. That way, you can give the password out only to those who have replied and seem credible.

To password-protect a meeting, start by scheduling a meeting and checking the box next to Require meeting password. It's only an option when you generate a unique ID, not when you use your PMI. You'll see a numeric password, which will work for everyone who has it.

**3. Create a Waiting Room**

A Zoom call can start one of two ways. It can start the moment the first person logs onto the call, or it can start when the host says it should start. For small groups of people who know each other, it's common for people to log in and make small talk while waiting for everyone else to join. Sometimes you want to let them chit-chat. For other calls, however, you might not want participants to chat with each other or even let the call officially start until you, the host, have signed in and are ready.

In that second case, the solution is to create a Zoom Waiting Room. When participants log into the call, they see a Waiting Room screen that you can customize, and they aren't let into the call until you, the host, lets them in. You can let people in all at once or one at a time, which means if you see names you don't recognize in the Waiting Room, you don't have to let them in at all.

**4. Make Sure Only the Hosts Can Share Their Screen**

Don't let anyone hijack the screen during a Zoom call. To prevent it, make sure your settings indicate that the only people allowed to share their screens are hosts.

You can enable this setting in advance as well as during a call.

In advance, go to the Zoom web portal (not the desktop app) and in the settings navigate to Personal > Settings > In Meeting (Basic) and look for Screen sharing. Check the option that only the host can share.



During a call, you can prevent others from sharing their screens by,using the host controls at the bottom. Click the up-facing carrot next to Share Screen. Choose Advanced Sharing Options and choose to only let the host

While sharing your screen or an image, Zoom has a great feature that lets participants annotate what they see. For visual collaboration, it's amazing. For naughty participants, it might seem like an invitation to bomb your call. You can disable the annotation feature in the In Meeting (Basics) section of your web account.

## 5. Create an Invite-Only Meeting

*This feature is for paid Zoom accounts only.*

One way to restrict who can join your Zoom call is to make it an invite-only meeting. That means the only people who can join the call are those you invited, and they must sign in using the same email address you used to invite them. It gives you much more assurance that people are who they say they are.

There are a few ways you can [enforce an invite-only meeting](https://support.zoom.us/hc/en-us/articles/360037117472-Authentication-Profiles-for-Meetings-and-Webinars?zcid=1231), depending on the type of account you have. The long and short of it is to look for an option called Authentication Profiles.

Once you have that setting enabled, anyone else who tries to join your meeting will see a notification on screen telling them that the meeting is for authorized attendees only.

## 6. Lock a Meeting Once It Starts

If you start a meeting and everyone you expect to join has, you can lock the meeting from new participants. While the meeting is running, navigate to the bottom of the screen and click Manage Participants. The Participants panel will open. At the bottom, choose More > Lock Meeting.

## 7. Kick Someone Out or Put Them on Hold

Sometimes an unruly participant manages to slip through the cracks. As the meeting host, you do have the power to kick someone out of a call or put them on hold.

## 8. Disable Someone's Camera

Hosts can turn off any participant's camera. If someone is being rude or inappropriate on video, or their video has some technical problem, the host can open the Participants panel and click on the video camera icon next to the person's name.

## 9. Prevent Animated GIFs and Other Files in the Chat

In the chat area of a Zoom meeting, participants can share files, including images and animated GIFs—if you let them. If you'd rather not, then be sure to disable file transfer. It's on by default, so you have to actively disable it.

For your own meetings, open Settings in the Zoom web app (it's not in the desktop app). On the left side, go to Personal > Settings. Then click In Meeting (Basic). Scroll down a little farther until you see File Transfer. That's where you can disable it.