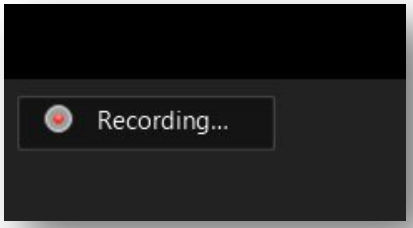
Securing your Zoom meetings

The FBI released an advisory warning Zoom users that they should properly secure their browsers from Zoom-bombing attacks.

> Zoom-bombing is when someone gains unauthorized access to a Zoom meeting to harass the meeting participants in various ways to spread hate and divisiveness, or to record pranks that will be later shown on social media.

Privacy considerations when using Zoom

One of the most important things to remember is that a Host can record a Zoom session, including the video and audio, to their computer. Therefore, be careful saying or physically 'revealing' anything that you would not want someone else to potentially see or know about.



Meeting participants will know when a meeting is being recorded as there will be a 'Recording...' indicator displayed in the top left of the meeting as shown.

A user can download their chat logs before leaving a meeting. These logs will only contain messages that you could see, but not the private chat messages of other users.

It's important to note that only the communication between a meeting participant and Zoom's servers is encrypted, while the related meeting data traversing over Zoom's network is not.

This theoretically means that a Zoom employee could monitor a meeting's traffic and snoop on it, but Zoom has reported that there are safeguards in place to prevent this type of activity.

Securing your Zoom meetings

Before scheduling a meeting with friends or coworkers, you need to familiarize yourself with the various ways to secure Zoom meetings using the following tips:

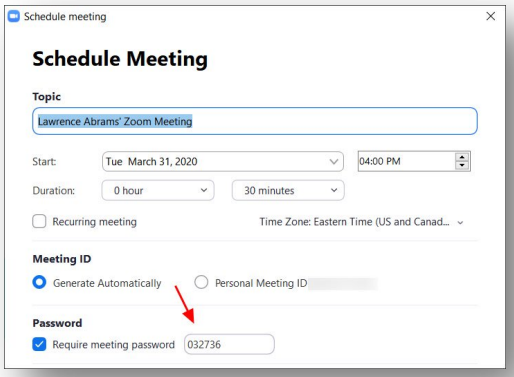
1. Add a Password to All Meetings
2. Use Waiting Rooms
3. Disable "Join Before Host"
4. Do Not Share Your Meeting ID
5. Disable Participant Screen Sharing
6. Lock Meetings When Everyone Has Joined
7. Do not Post Pictures of Your Zoom Meetings
8. Do Not Post Public Links to Your Meetings
9. Keep Zoom Client Updated
10. Be on the Lookout for Zoom-Themed Malware

We've also included five advanced security tips in this document.

Add a password to all meetings!

When creating a new Zoom meeting, Zoom will automatically enable the "Require meeting password" setting and assign a random 6-digit password.

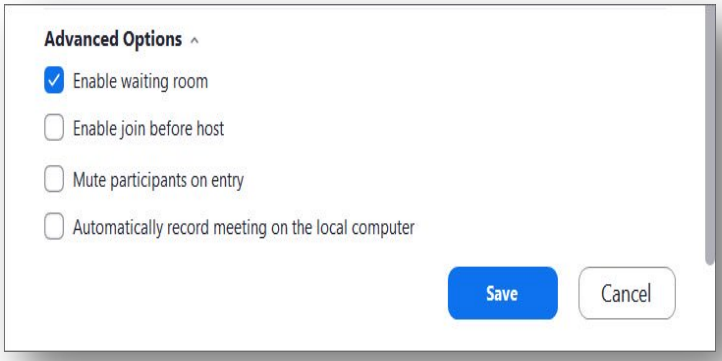
You should not uncheck this option as doing so will allow anyone to gain access to your meeting without your permission.



(return to top)

Use waiting rooms

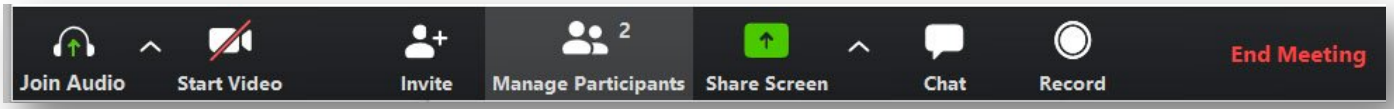
Zoom allows the host (the one who created the meeting) to enable a waiting room feature that prevents users from entering the meeting without first being admitted by the host.



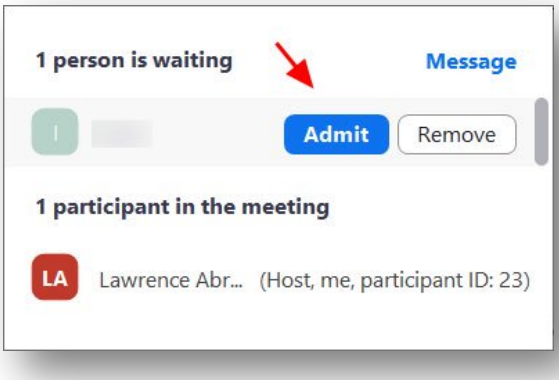
This feature can be enabled during the meeting creation by opening the advanced settings, checking the 'Enable waiting room' setting, and then clicking on the 'Save' button.

When enabled, anyone who joins the meeting will be placed into a waiting room where they will be shown a message stating "Please wait, the meeting host will let you in soon."

The meeting host will then be alerted when anyone joins the meeting and can see those waiting by clicking on the 'Manage Participants' button on the meeting toolbar.



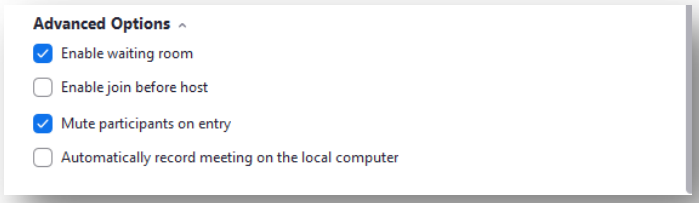
You can then hover your mouse over each waiting user and 'Admit' them if they belong in the meeting.



(return to top)

Disable "Join before Host"

The Join Before Host option can be convenient for allowing others to continue with a meeting if you are not available to start it, but with this option enabled, the first person who joins the meeting will automatically be made the host and will have full control over the meeting. (return to top)



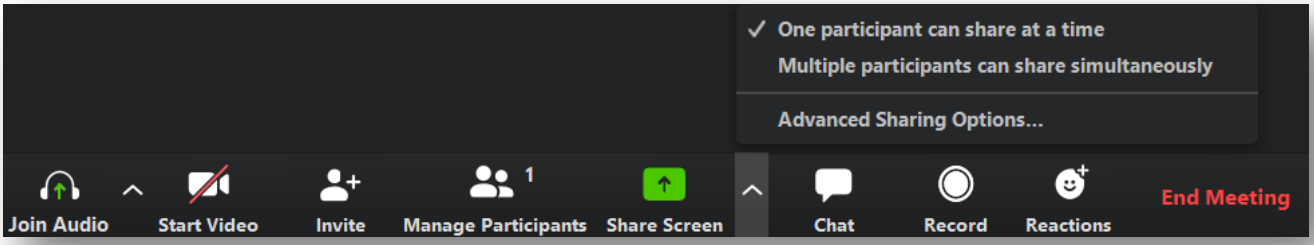
Do not share your meeting ID

Each Zoom user is given a permanent 'Personal Meeting ID' (PMI) that is associated with their account.
If you give your PMI to someone else, they will always be able to check if there is a meeting in progress and potentially join it if a password is not configured.
Instead of sharing your PMI, create new meetings each time that you will share with participants as necessary. (return to top)

Disable participant screen sharing

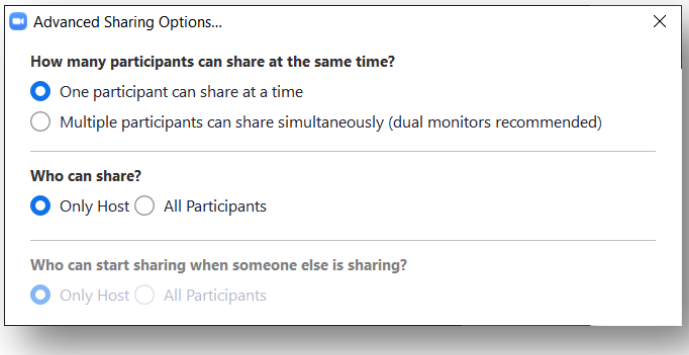
To prevent your meeting from being hijacked by others, you should prevent participants other than the Host from sharing their screen.

As a host, this can be done in a meeting by clicking on the up arrow next to 'Share Screen' in the Zoom toolbar and then clicking on 'Advanced Sharing Options' as shown below.



When the Advanced Sharing Options screen opens, change the 'Who Can Share?' setting to 'Only Host'.

You can then close the settings screen by clicking on the X.



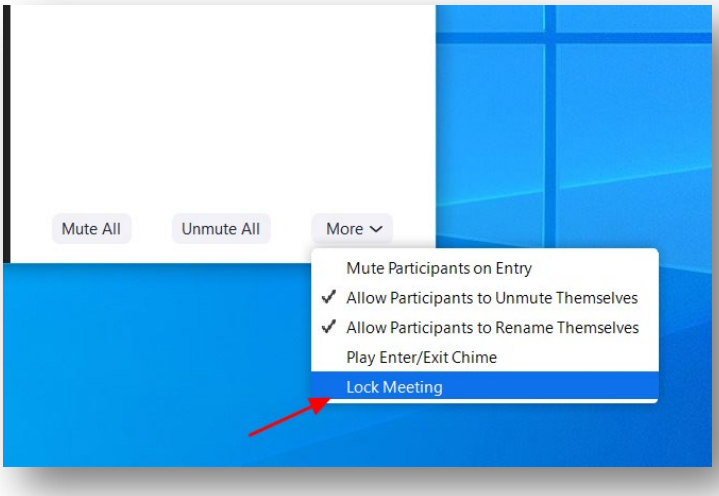
(return to top)

Lock meetings when everyone has joined

If everyone has joined your meeting and you are not inviting anyone else, you should Lock the meeting so that nobody else can join.

To do this, click on the 'Manage Participants' button on the Zoom toolbar and select 'More' at the bottom of the Participants pane. Then select the 'Lock Meeting' option as shown below.

This is also where you can 'Mute Participants on Entry' and set whether participants can unmute themselves. (return to top)

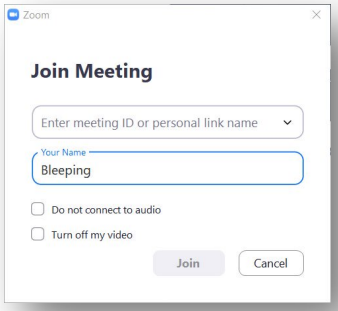


Do not post pictures of your Zoom meetings

If you take a picture of your Zoom meeting than anyone who sees this picture will be able to see its associated meeting ID. This can then be used by uninvited people to try and access the meeting. For example, the UK Prime Minister Boris Johnson tweeted a picture of the "first even digital Cabinet" and included in the picture was the meet ID.

This could have been used by attackers to try and gain unauthorized access to the meeting by manually joining via the displayed ID.

Thankfully, the virtual cabinet meeting was password-protected but does illustrate why all meetings need to use a password or at least a waiting room.



(return to top)

Do not post public links to your meetings

When creating Zoom meetings, you should never publicly post a link to your meeting.

Doing so will cause search engines such as Google to index the links and make them accessible to anyone who searches for them.

As the default setting in Zoom is to embed passwords in the invite links, once a person has your Zoom link they can Zoom-bomb your meeting. (return to top)

Keep Zoom client updated

If you are prompted to update your Zoom client, please install the update.

The latest Zoom updates enable Meeting passwords by default and add protection from people scanning for meeting IDs.

With Zoom being so popular at this time, more threat actors will also focus on it to find vulnerabilities. By installing the latest updates as they are released, you will be protected from any discovered vulnerabilities. (return to top)

Be on the lookout for Zoom-themed malware

Since the Coronavirus outbreak, there has been a rapid increase in the number of threat actors creating malware, phishing scams, and other attacks related to the pandemic.

This includes malware and adware installers being created that pretend to be Zoom client installers.
To be safe, only download the Zoom client directly from the legitimate Zoom.us site and not from anywhere else

(return to top)

Advanced Security Recommendations

- **Embed password in meeting link for one-click join**
  Meeting password will be encrypted and included in the join meeting link to allow participants to join with just one click without having to enter the password.

- **Mute participants upon entry**
  Automatically mute all participants when they join the meeting. The host controls whether participants can unmute themselves

- **Prevent participants from saving chat**

- **Allow host to put attendee on hold**
  Allow hosts to temporarily remove an attendee from the meeting.

- **Disable desktop/screen share for users**
  Disable desktop or screen share in a meeting and only allow sharing of selected applications.

Additional resources

- Security at Zoom https://zoom.us/security

- FBI Warning: https://www.fbi.gov/contact-us/field-offices/boston/news/press-releases/fbi-warns-of-teleconferencing-and-online-classroom-hijacking-during-covid-19-pandemic

(return to top)