Zoom Security

Introduction

Zoom is a wonderful system for video conferencing and sharing. Senior Planet was able to move their classes online via Zoom in March 2020. This was done in an amazing short amount of time. This has allowed more people from more places to take advantage of Senior Planet which had been limited to a small number of geographic regions in the United States.

Unfortunately, along with the rapid popularity of the Zoom platform, some serious security issues quickly became apparent. People called "Zoom Bombers" got into many meeting, particularly school sessions and did some very disturbing things.

Zoom spent three months in early 2020 improving the security of their system and the current Zoom system is much more secure now than at the beginning of the pandemic.

Basic Security Features

Zoom has always had a number of security features but the early versions of Zoom did not require using them and the default settings did not have these enabled.

When you are scheduling a meeting, you will see this as part of the form:

Security	☑ Passcode 342126
	Only users who have the invite link or passcode can join the meeting
	☐ Waiting Room
	Only users admitted by the host can join the meeting
	☐ Require authentication to join

You are required to choose at least one of these three options (Passcode, Waiting Room, User Authentication) which are described below.

You can also change the passcode for the meeting with this part of the form if you decide to use a passcode.

Meeting ID

Each meeting has a meeting ID associated with it. Every user with a Zoom account (free or paid) is given a personal meeting ID. When you schedule a meeting or start a meeting without scheduling it, you have the choice to use your personal ID or have Zoom create a unique ID for your meeting.

It is normally a good idea to use a unique ID for each meeting that you schedule, but you can use your personal ID for unscheduled meetings if you like. Any meeting you start with your personal ID will have the same meeting ID (and passcode) and therefore the same Zoom link.

When you schedule a meeting, this is the option that determines if the meeting will use your personal meeting ID (PMI):

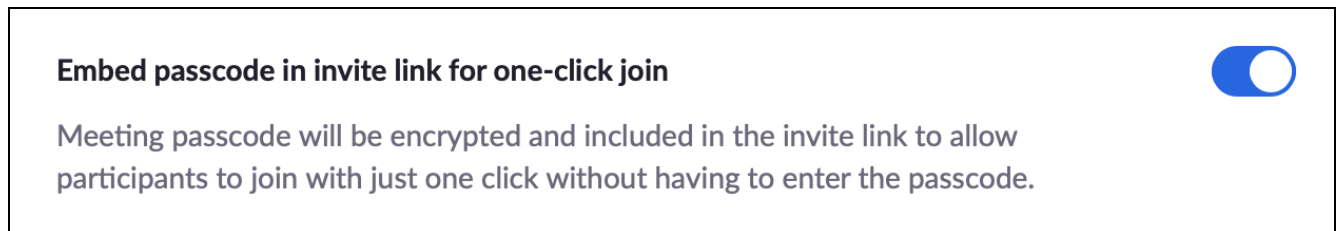| Meeting ID	● Generate Automatically	○ Personal Meeting ID 476 591 1917

Passcodes

Every Zoom meeting can have an optional passcode (aka. password) that either must be entered manually or can be embedded in the Zoom link. This is done with a **"?pwd="** in the Zoom link followed by an encrypted version of the passcode. You specify in your Zoom settings whether to use a passcode for a meeting and also whether to embed the passcode in the link.

For example, the link for the Apple Addicts sessions is:

https://seniorplanet.zoom.us/j/95473978676?pwd=ZFdUWFk3b3ZXSFVRaTBiRHNmTC93QT09

The meeting ID is the part after the **"/j/"** (**95473978676**) and the encrypted passcode is the part after the **"?pwd="** (**ZFdUWFk3b3ZXSFVRaTBiRHNmTC93QT09**)

When you schedule a meeting, you get to decide whether to embed the passcode in the meeting link:

Embed passcode in invite link for one-click join

Meeting passcode will be encrypted and included in the invite link to allow participants to join with just one click without having to enter the passcode.

Whether or not to embed the passcode in the link is a tradeoff of convenience versus some extra security. If the passcode is not in the link, the participant must know both the Zoom meeting ID and the passcode and enter both to join the meeting.

If you are simply setting up a meeting with friends and not publishing the Zoom link on a website, it is perfectly reasonable to include the passcode in the link so that your participants only need to click on the meeting link to join the meeting.

On the Zoom website, you can click on Settings and then in the Meetings section you change the passcode for meetings that use your personal meeting ID:

Personal Meeting ID (PMI) Passcode

All Personal Meeting ID (PMI) meetings that users can join via client, or room systems will be passcode-protected.

Passcode: ****** Show Edit

If you click on the Edit link, you can change the passcode for the meeting:

Personal Meeting ID (PMI) Passcode

All Personal Meeting ID (PMI) meetings that users can join via client, or room systems will be passcode-protected.

Passcode: 876123 Save Cancel

Waiting Room

Another option is to use a waiting room for your meeting. This means the meeting host (or a co-host) needs to approve each participant before they can join the meeting. The Waiting Room is displayed at the top of the Participants window for the host and co-host and they need to accept individual participants or they can click a link to accept all people in the Waiting Room.

The waiting room option is a good idea if you publish the meeting link on a website. This prevents Zoom Bombers from joining the meeting without your knowlege. The Lunch and Learn meetings use a waiting room but only the host and co-hosts can see it.

The Waiting Room section is at the top of the Participants window which is displayed by clicking the Participants button:
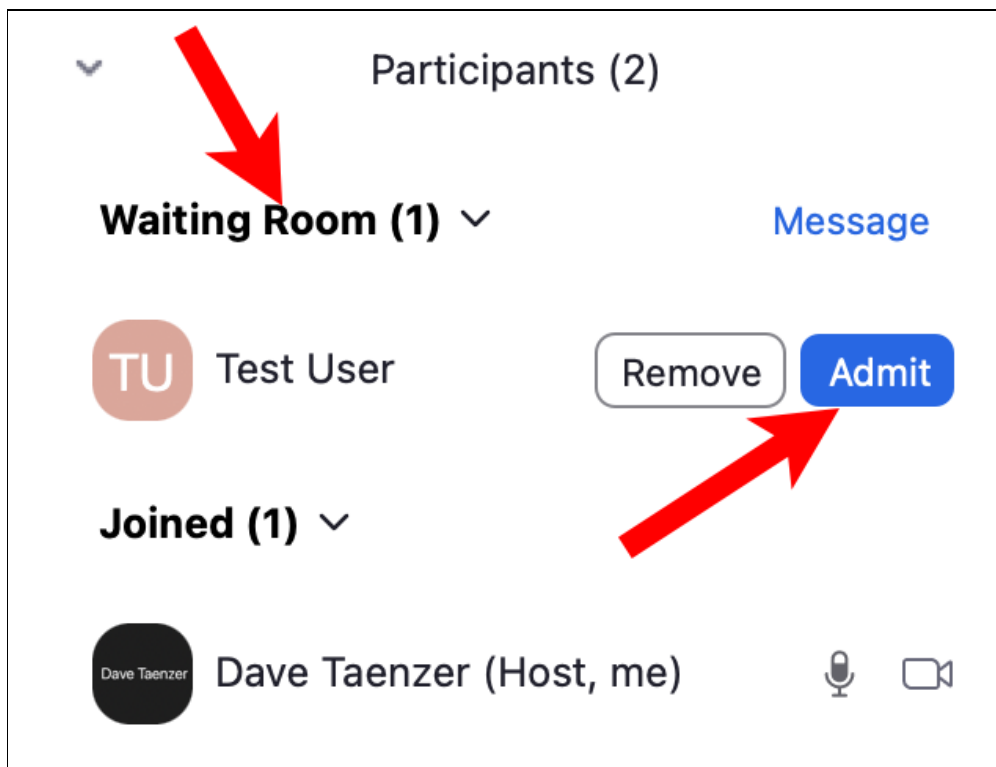
User Authentication

You can also specify that only authenticated users (who are logged into Zoom) can join the meeting. With business accounts, you can limit the email addresses of your participants to only the company accounts.

This means that people that want to join the meeting must have a Zoom account and log into it before they join the meeting or they will need to do this when they try to join it.

This can be useful if you want to make sure that your participants are properly identified but can be a problem if your attendees don't have a Zoom account (or know how to log in with a Google Account).

We don't currently use this on Lunch and Learn to try to keep it as simple as possible to join the meetings.

Meetings That Require Registration

If you have a paid Zoom account, you can require that all participants register for your meeting and also control whether the registrations are automatically accepted or must be manually accepted by you.

Each participant who registers is given a unique Zoom link that identifies them when they enter the meeting so you should tell people who register not to give the link to other people but ask them to register too.

You can also specify a set of questions that people are asked when they register and control which questions are mandatory and which ones are optional.

This is a bit more complicated process and there is a video in the Resources section below that explains the registration options.

In Meeting Security Options

When you are in a Zoom meeting as host or co-host, you will see a Security button at the bottom of the window:
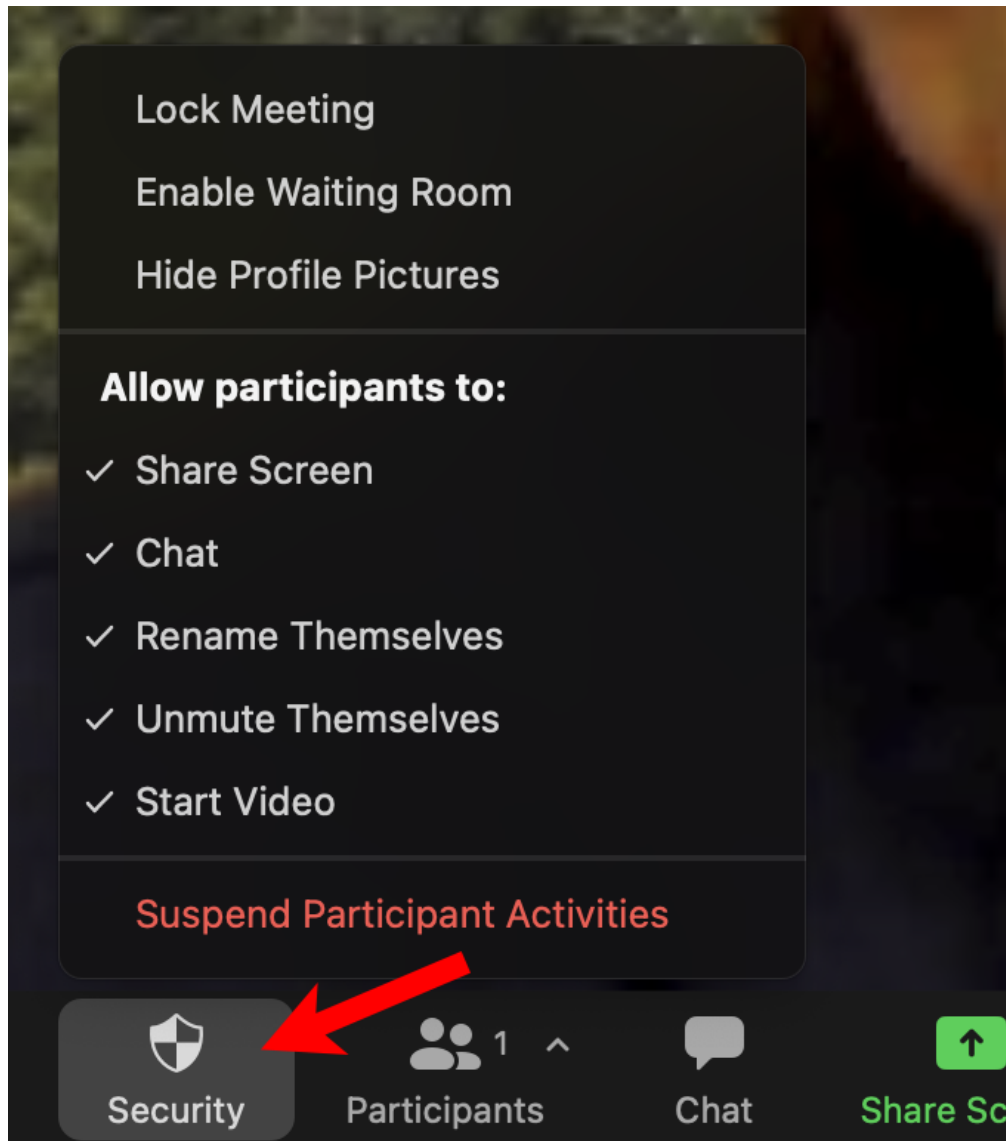

There are options to stop all participant activities, lock the meeting (from letting in new people) and control what each participant can do (e.g. share screen, unmute themselves and start video).

You can also control the options for a single user by clicking on the three dot menu button in the upper right part of their picture on the screen:
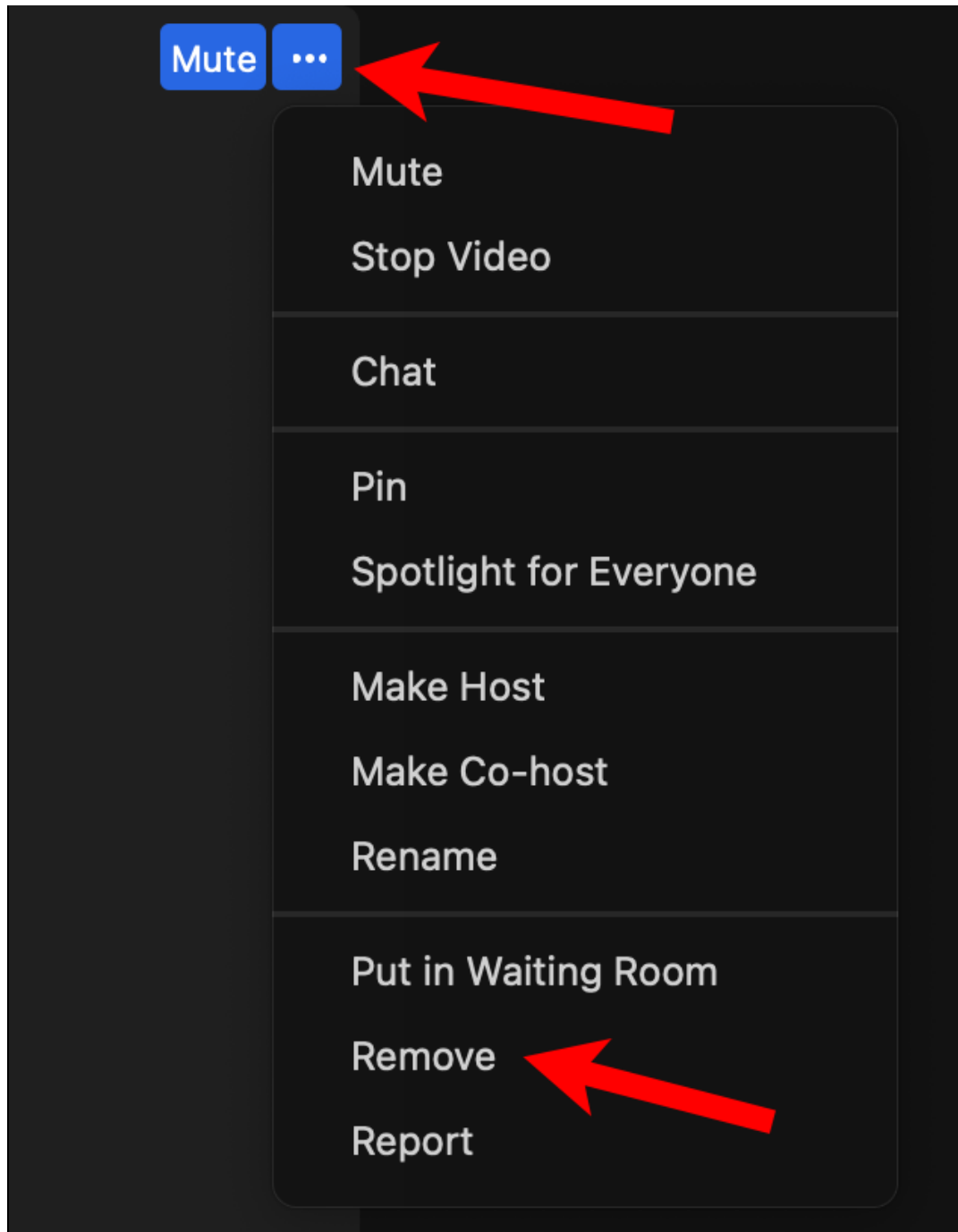

One useful option is to immediately remove them from the meeting with the Remove option.

These options are also available in the Participants window by clicking on the blue More button to the right of their name:
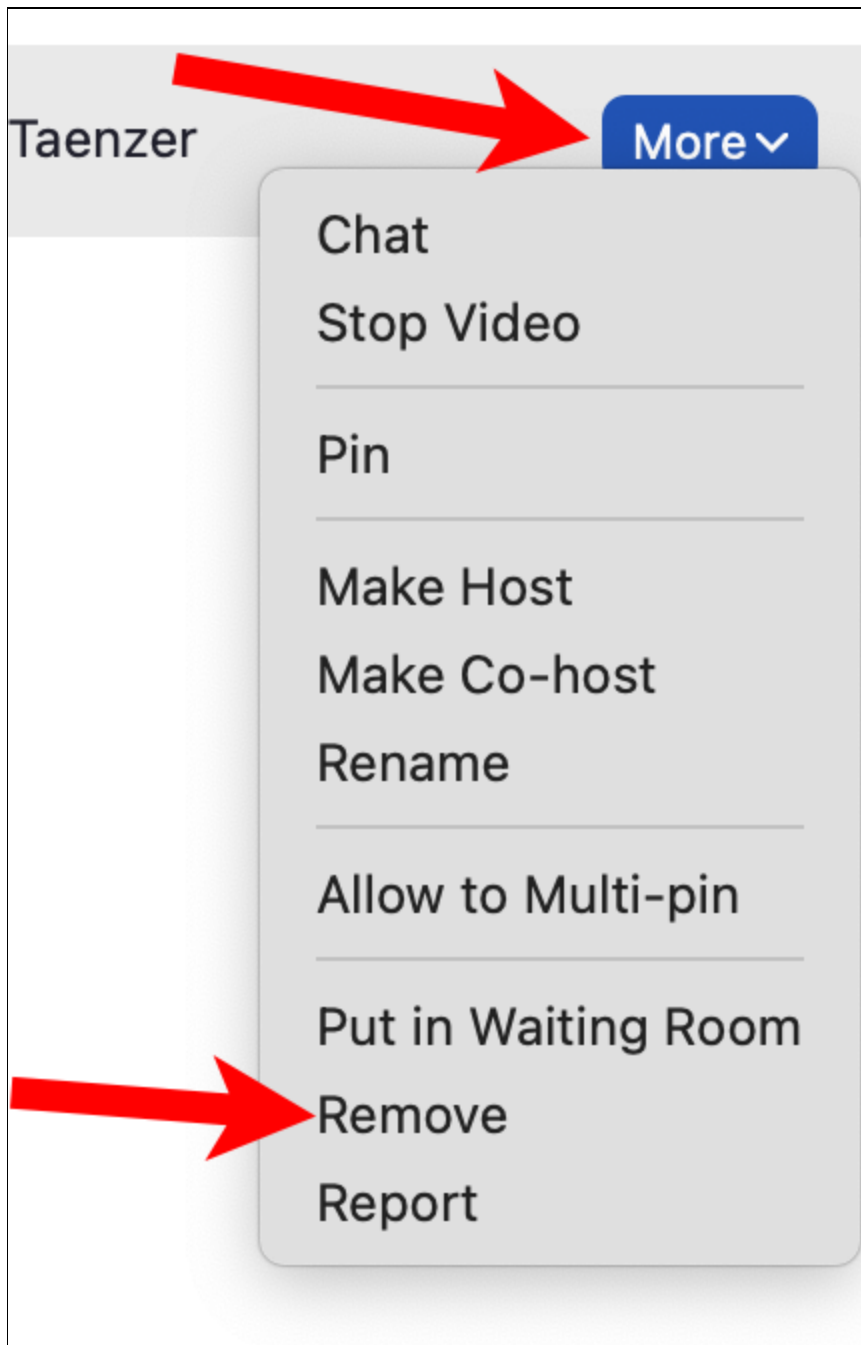

This is also the menu you can use as host to make specific participants co-hosts or transfer the host status to a participant.

Next to the three dot menu at the top right corner of each user picture is a Mute button:
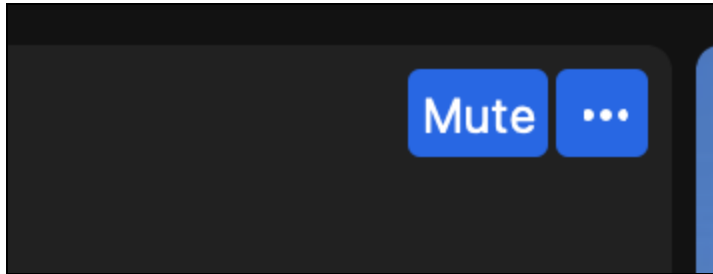

Which you can use to quickly silence a user who is misbehaving or accidentally generating background noise.

After you mute a user, you see a button to ask them to unmute themselves:
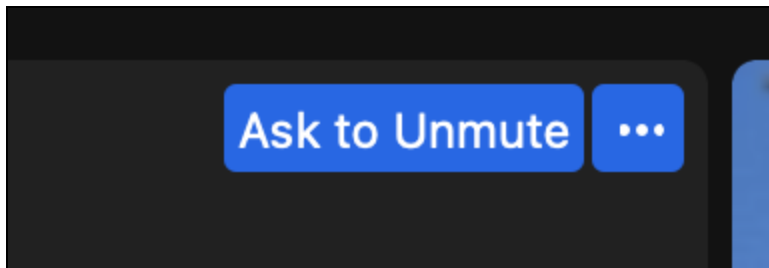
Preventing Chat Bombers

Another thing you can do to prevent Zoom Bombers from inappropriate chat messages is to limit who people can chat with. Click the three dot button in the bottom right of the chat window to see this menu:
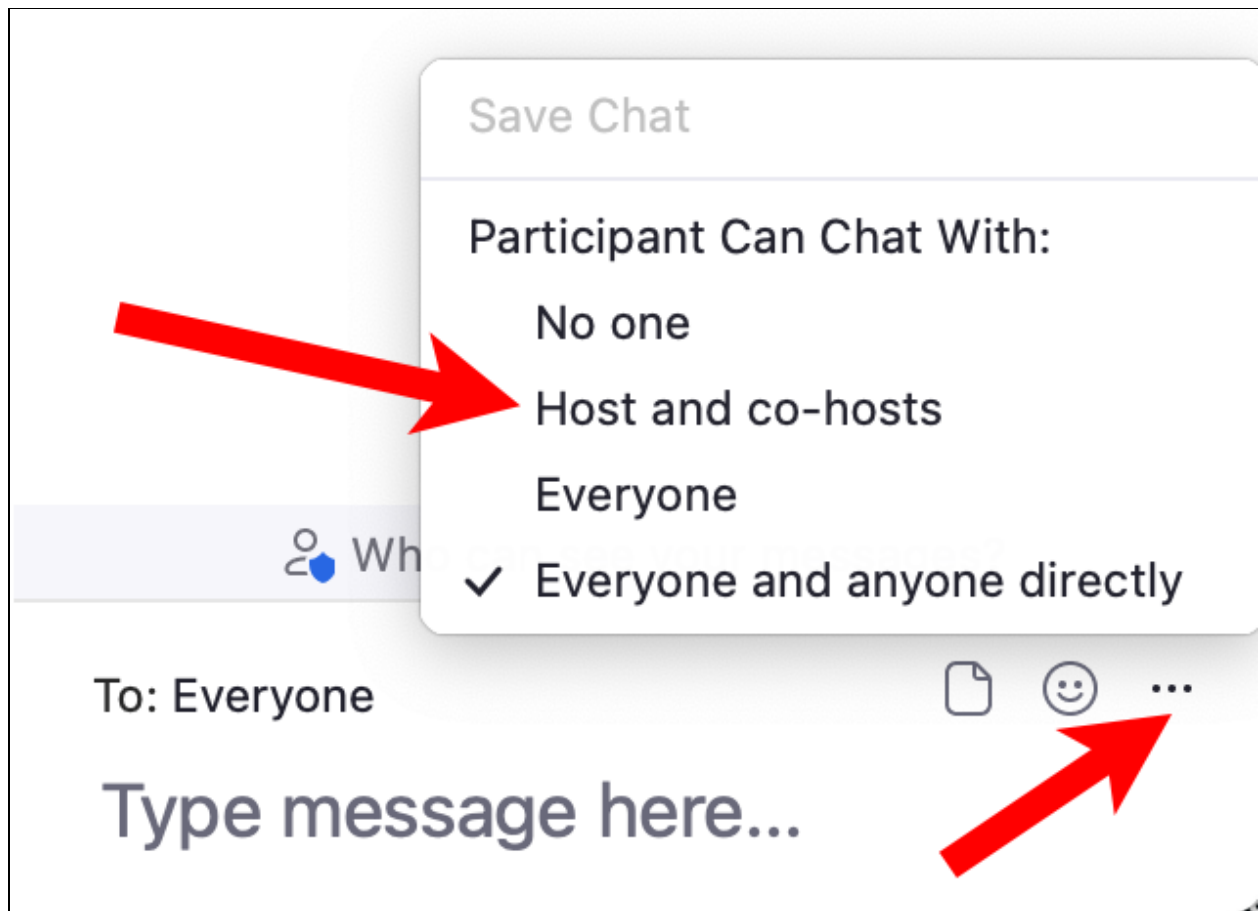
For Lunch and Learn sessions, we are limiting participants to sending chat messages to the host and co-hosts.

Unfortunately we will probably have to continue to use this setting for the time being.

What You Can Do to Help As a Co-host

If you volunteer to help with security in a meeting, the host can make you a co-host. This gives you permission to

- Help accept people into the meeting from the waiting room

- Mute people who are making background noise

- Lower the hand of people who have raised their hand

- Send chat messages to everyone in the meeting

- Mute a person who is misbehaving

- Turn of the camera of a person who is misbehaving

- If necessary remove Zoom Bombers from the meeting

The host will instruct you on which items they would like you to help them with. Often this will be letting people into the meeting and muting people generating accidental background noise.

Dealing with Zoom Bombers will probably be done by the host and not a co-host. You have the power to do this but you should probably leave this decision to the host running the meeting.

Conclusions

Zoom provides many security options. Some of these are choices you make when you schedule a meeting and others are used after the meeting starts.

If you do get Zoom Bombers in your meeting that are trying to disrupt it, you can prevent them from using the chat to send messages to everyone. You can also mute them, turn off their video, remove them from the meeting and also report their misbehavior.

The combination of these security measures will make Zoom Bombing much less likely and give you the necessary tools to deal with these people if necessary.

Resources

Zoom Trust Center

https://explore.zoom.us/en/trust/

In meeting security options

https://support.zoom.us/hc/en-us/articles/360041848151-In-meeting-security-options

Scheduling a Meeting with Registration

https://support.zoom.us/hc/en-us/articles/211579443-Scheduling-a-meeting-with-registration

Configuring authentication settings and profiles

https://support.zoom.us/hc/en-us/articles/360037117472-Configuring-authentication-settings-and-profiles

Zoom Meeting Registration Video

https://www.youtube.com/watch?v=F927modarHY