



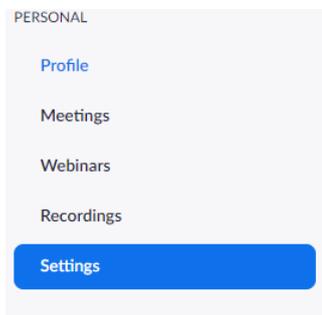
Online Zoom Meeting Hosting Guidelines

Purpose: to protect everyone’s anonymity, ensure smooth running of meetings, protect data & privacy.

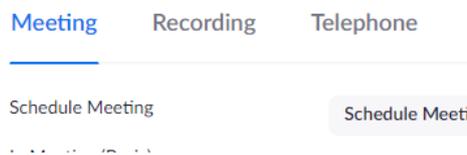
1. Zoom settings

(needs to be done only once per account prior to setting up a meeting, not before every meeting)

- a. On the Zoom website, log in with the account you use to host meetings
- b. Navigate to: Settings



- c. In the Zoom Settings section, under the Meetings subtab enable/disable the following options:



- **Enable: Require Encryption for Third Party Endpoints** *(privacy protection)*

Require Encryption for 3rd Party Endpoints (H323/SIP)

Zoom requires encryption for all data between the Zoom cloud, Zoom client, and Zoom Room. Require encryption for 3rd party endpoints (H323/SIP).





- **Disable: Auto saving chats** *(anonymity and privacy protection)*

Auto saving chats

Automatically save all in-meeting chats so that hosts do not need to manually save the text of the chat after the meeting starts.



- **Disable: File transfer** *(protect against potential copyright infringement or sharing of indecent content)*

File transfer

Hosts and participants can send files through the in-meeting chat.



- **Disable: Feedback to Zoom** *(privacy protection)*

Feedback to Zoom

Add a Feedback tab to the Windows Settings or Mac Preferences dialog, and also enable users to provide feedback to Zoom at the end of the meeting



- **Disable: remote control** *(anonymity and privacy protection)*

Remote control

During screen sharing, the person who is sharing can allow others to control the shared content



- **Disable: Virtual Background**

Virtual background

Allow users to replace their background with any selected image. Choose or upload an image in the Zoom Desktop application settings.



- **Enable: Screen Share for Host only** *(disruption, data protection)*

Screen sharing

Allow host and participants to share their screen or content during meetings



Who can share?

Host Only All Participants

Who can start sharing when someone else is sharing?

Host Only All Participants

- **Enable: Disable desktop/screen share for users**

Disable desktop/screen share for users

Disable desktop or screen share in a meeting and only allow sharing of selected applications.



- **Disable: Annotation**

Annotation

Allow participants to use annotation tools to add information to shared screens



- **Disable: Whiteboard**

Whiteboard

Allow participants to share whiteboard during a meeting





- **Enable: Co-Host feature** *(during meeting host can assign co-host)*

Co-host

Allow the host to add co-hosts. Co-hosts have the same in-meeting controls as the host.



- **Enable: Blur snapshot on iOS task switcher** *(anonymity and privacy protection)*

Blur snapshot on iOS task switcher

Enable this option to hide potentially sensitive information from the snapshot of the Zoom main window. This snapshot display as the preview screen in the iOS tasks switcher when multiple apps are open.



- **Enable: Show a “Join from browser” link**

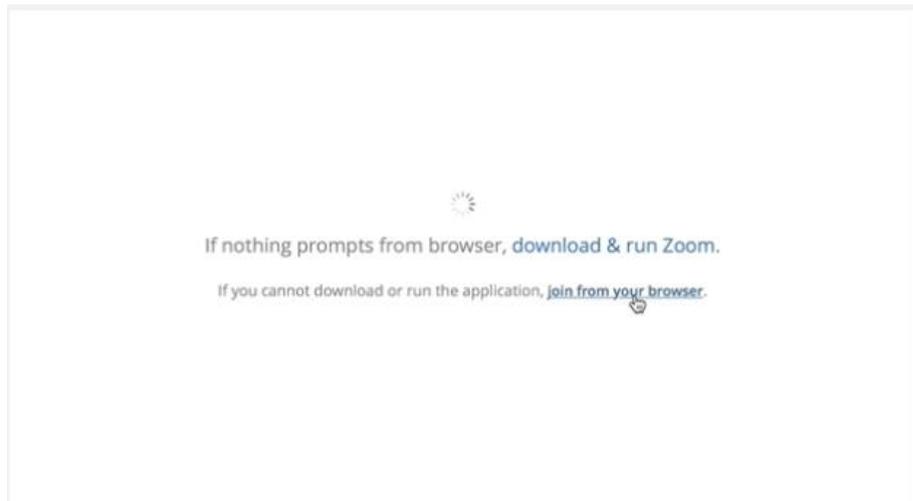
For individuals who cannot install any software on their work computer i.e. commission workers, meetings via this option may work unless further preventative measures are installed on the computer

Show a "Join from your browser" link

Allow participants to bypass the Zoom application download process, and join a meeting directly from their browser. This is a workaround for participants who are unable to download, install, or run applications. Note that the meeting experience from the browser is limited



When a participant clicks the meeting URL, instead of clicking download & run Zoom they should click **join from your browser**.



- d. In the Zoom Settings section, under the Recordings subtab enable/disable the following options:





- **Disable: Local recording** *(anonymity and privacy protection)*
- **Disable: Cloud recording** *(anonymity and privacy protection)*
- **Disable: Automatic recording** *(anonymity and privacy protection)*

Local recording

Allow hosts and participants to record the meeting to a local file



Cloud recording

Allow hosts to record and save the meeting / webinar in the cloud



Automatic recording

Record meetings automatically as they start



e. In the Zoom Settings section, under the Telephone subtab enable/disable the following options:

Meeting Recording **Telephone**

- **Enable: Mask phone number in the participant list** *(anonymity and privacy protection)*

Mask phone number in the participant list

Phone numbers of users dialing into a meeting will be masked in the participant list. For example: 888****666





2. Meeting Setup

- Topic
 - Choose a meeting name that preferably does not include AA. This is for added anonymity if attending meetings in public spaces
- Disable: Registration
- Password: enabled by default
- Video:
 - Enable Video OFF for Host and Participants (it means video is switched off when host or participant joins the meeting but can be turned on after that)
- Audio:
 - Enable: Both
 - Click **Edit** to update the country list
- Meeting Options:
 - Disable: Enable join before host (*This prevents people from joining the group before a host logs in. See “Enable Waiting Room”*)
 - Enable: Mute participants upon entry
 - Enable: Enable Waiting Room (*helps you see who is trying to enter your meeting by placing them in a separate area at the top of your participants list until you let them into the main meeting. It also prevents you from getting flooded with disruptive people because it gives you a pre-emptive chance to see who is trying to enter your meeting. Wouldn't it be nice to be able to stop someone from naming themselves, say, “GateKrasherFU” or keep known bad actors from even entering your meeting at all in the first place? Waiting Room let's you do just that. You're not going to catch everybody, of course but even that occasional bad actor that does get in won't be able to unmute themselves, upload files, take over screen share or chat anyway. And who knows, maybe they might even get sober? Of course, nothing prevents them from raising their hand and once called upon to start their obscene gibberish, but at least it's only one person, very easy to ban and not let back in for the rest of the meeting. Just like what happens at real meetings sometimes.*)
 - Disable: Only authenticated users can join



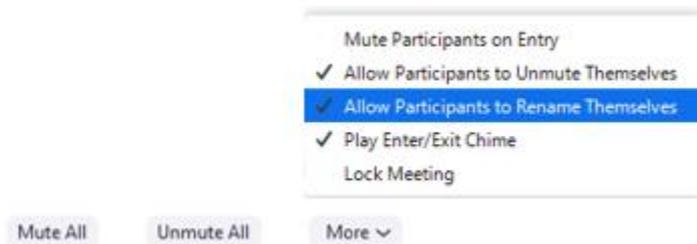
3. Suggested practices during a meeting

- **Ask someone to be Co-Host**

Depending on the size of the meeting we suggest to have up to two co-hosts. Select their name in the participant list, click on MORE and make them co-host. They can keep an eye on the participant box & chat with you and help manage against an attack. Two or more people acting calmly and fast is better than one.

- **Disable: User Rename** (*disruption*)

A bad actor can post something nasty in your chat and then quickly rename themselves. Their posted chat will retain the old name but they will already be cloaked with their new name as you try to find them and ban them.



- **Video participation and names** (*anonymity*)

Some may not have their video on. Others may show their full name in the participant box unintentionally. Using Video is not compulsory and participants are free to use whatever name they please. We suggest participants use video for an immersive experience for everyone.

We suggest participants type their first name into the system when they join. It can be checked on their own screen and in the participant list. We suggest the host say and/or writes via chat message before meeting starts :

“Using video during the meeting is your personal choice. We encourage you to enable video for a better meeting experience. We ask that you use your first name as your participant name, check your Zoom screen and/or participant box for your current username. Especially if it shows 'iphone' 'samsung' ... etc., contact the host via the chat box or introduce yourself before the meeting requesting the host to rename you. The rename feature has been disabled for participants for security reasons. Before your next meeting we encourage you to learn how to name yourself ahead of joining. Here is a short How-To guide <https://bit.ly/34r1ES7>.”



● Participation calls via Landline

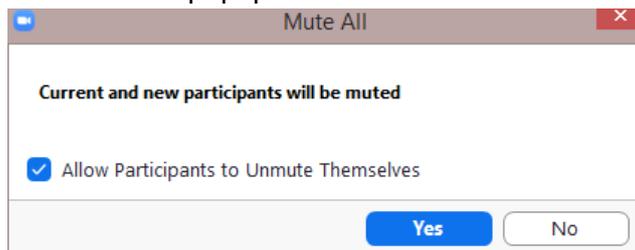
Dialed in participants may not be able to mute/unmute themselves because their (landline) phone doesn't support it or they may be visually impaired. It is suggested that hosts ask the caller whether they can unmute themselves. If not they stay unmuted if at all possible throughout the entire meeting or suggest to keep them muted until invited by the host to share. Definitely ask them to introduce themselves so you can rename them in the participant box.

4. What to do if a meeting is attacked

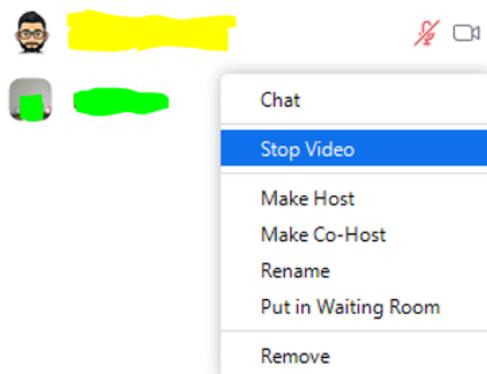
Expect explicit, obscene porn, lewd images, foul language and verbal abuse (often directed at the lead/chairperson to invoke chaos). First and foremost, remain calm, having expected to experience this. Shock is their primary goal. If you are calm, you can act quickly and decisively instead of react.

Having already blocked their ability to video-share and send files which is their primary weapon, the only thing that intruders can do now is post in the chat, show live video from their device, and/or verbally abuse, which they seem to like to do in gangs of many in order to rapidly overcome a meeting. Depending on whether the abuse is mainly verbal or video start taking action:

- 1. **Mute ALL** quickly go over to the participant list and immediately click the "Mute All" button. In the popup window unselect 'Allow Participants to Unmute Themselves'.



- 2. **Stop their video** go to the participant list and click MORE on their name (if their main offence is video you may want to do this first)



- 3. Click the **Security** button at the bottom of your Zoom Window



	<ul style="list-style-type: none">- ENABLE Lock Meeting- DISABLE Chat- DISABLE Rename Themselves- REMOVE Participants<ul style="list-style-type: none">- This will add a red REMOVE button next to each participant in the participant list <table border="0"><tr><td></td><td></td><td>Remove</td></tr><tr><td></td><td></td><td>Remove</td></tr><tr><td></td><td></td><td>Remove</td></tr></table>			Remove			Remove			Remove
		Remove								
		Remove								
		Remove								

4. This essentially gives Zoom-bombers no reason to stay on at this point, and they likely will start dropping once they see that you know how to take away their ability to disrupt a meeting. Under normal meeting circumstances, you want members to be able to mute and unmute themselves in order to engage more naturally with the group as we would in face-to-face meetings, so blocking attendees from unmuting themselves should be a temporary action until the intruders have left.
5. Feel free at any time, unmuting yourself and your co-hosts, to inform the audience what you're doing (while attendees remain force-muted, things tend to get awkward), putting a temporary hold on the meeting while the problem is being addressed. Let them know to **please raise their hand** if they wish to speak and that the meeting will restart shortly.
6. During this hold period, have your co-host(s) along with you, click on "Participants", go through and "**Remove**" all the obviously bad actors. You can also distinguish most of them from the names or images they post for themselves. Sometimes they will have video on, being their only chance left to show a shock video, with the camera pointing somewhere random like a ceiling fan. If you are unsure and don't want to drop someone who may be an actual AA member, unmute them and request that they identify themselves. Trolls either won't identify or they will say something making it obvious they are a troll, or they'll just stay silent or drop altogether.
7. Once you've experienced this a few times, it will be easier and troll groups will find your meeting "no fun" and will move on. If we get enough of our groups shutting them down, they will stop having any reason to Zoom-bomb our AA meetings.
8. Once all culprits have been successfully dealt with, feel free to allow participants to **unmute themselves** again and **re-enable the chat**.



9. Keep the meeting locked to prevent culprits from joining the meeting again. Anyone who wants to join and finds a meeting locked can communicate this in the WhatsApp group chat.

6. Resources

- 1) [How to Keep Uninvited Guests Out of Your Zoom Event](#)
- 2) [How to prevent your Zoom meetings being Zoom-bombed \(gate-crashed\) by trolls](#)
- 3) ['Zoombombing': When Video Conferences Go Wrong](#)