Guide to Securing your Zoom Meetings

The term "Zoom Bombing" refers to when an uninvited participant intentionally joins and disrupts a public Zoom, Skype, Hangouts, or other online meeting by sharing inappropriate images or audio.

It's important to understand that the uninvited participants did not "hack" Zoom to do this. They simply found the meeting information online and then disrupted the meeting because the host did not take any basic security precautions.

By protecting your meeting information and following basic security practices, you can ensure your Zoom meetings are safe, secure, and not vulnerable to "Zoom Bombing."

Follow these simple steps to ensure your Zoom meetings are secure:

1. Do not post your Meeting weblink or ID on a public website.

2. Do not share the Zoom meeting information on social media or in public forums.

3. When scheduling a meeting, require a password to join the meeting in addition to generating a unique meeting ID (never use your personal meeting ID for meetings).

4. Follow the detailed instructions in this guide to ensure your Zoom account is configured properly. This will ensure your meetings are secure, fully controlled by you, and not subject to disruption when you are meeting in a group environment.

Note: most of the settings described in this Guide require the latest version of the Zoom software. Be sure to update your Zoom software on your computer if prompted.

Zoom Security Guide

1. **Never use your Personal Meeting ID when creating a meeting**
   Because your Personal Meeting ID always remains the same, it would be easy for someone to save this information and join future meetings without your permission. Instead, generate a unique **Meeting ID** for all meetings to keep them secure.

   a. Under **Meetings > Schedule a Meeting > Meeting ID** select **Generate Automatically** each time you schedule a meeting.

   Meeting ID   ● Generate Automatically   ○ Personal Meeting ID

2. **Require a Meeting Password**
   For additional security, you can require participants to enter a password to join the meeting. Make sure you give the password to the meeting attendees in advance. Don't post passwords on websites or give them out publicly.

   a. Under **Meetings > Schedule a Meeting > Meeting Password** check **Require meeting password** and enter a password of your choosing.

   Meeting Password   ☑ Require meeting password   ••••••••••••

3. **Remove the "Enable Join Before Host" checkmark.**
   The **Enable join before host** option lets meeting attendees or students start the meeting without you being present. This should <u>never</u> be checked for meetings that involve students, as you don't want them to start a meeting without supervision. However, this option may be useful at times when you want a meeting to start even if the "host" (you) aren't present to start the meeting at the appointed time (such as a staff meeting).

   a. Under **Meetings > Schedule a Meeting > Meeting Options** remove the checkmark from the **Enable join before host** check box.

   Meeting Options   ☐ Enable join before host

4. **Enable the Waiting Room feature**
   This option prevents attendees from joining your meeting until you are ready for them. When an attendee connects to the meeting, you'll receive an alert. Admit them by selecting the **Admit** option in the Participants list. (Note: if enabled, this will automatically disable the "Enable join before host" option.)

   a. Under **Meetings > Schedule a Meeting > Meeting Options** check **Enable waiting room**

   b. When participants connect to the meeting, they will be asked to wait until you click on the **Admit** button next to their name in the **Manage Participants** list.
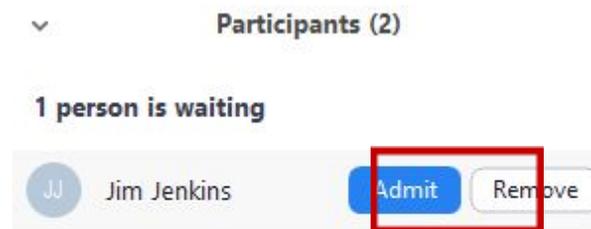

   c. You can read more information about Zoom Waiting Rooms here: https://support.zoom.us/hc/en-us/articles/115000332726-Waiting-Room

   d. You can enable the Waiting room feature by default. Navigate to your Zoom settings (https://zoom.us/profile/setting), select **In Meeting (Advanced)**, then enable the **Waiting Room** option (see below example). This setting will require the host to actively monitor the Participants to **Admit** people to the meeting.
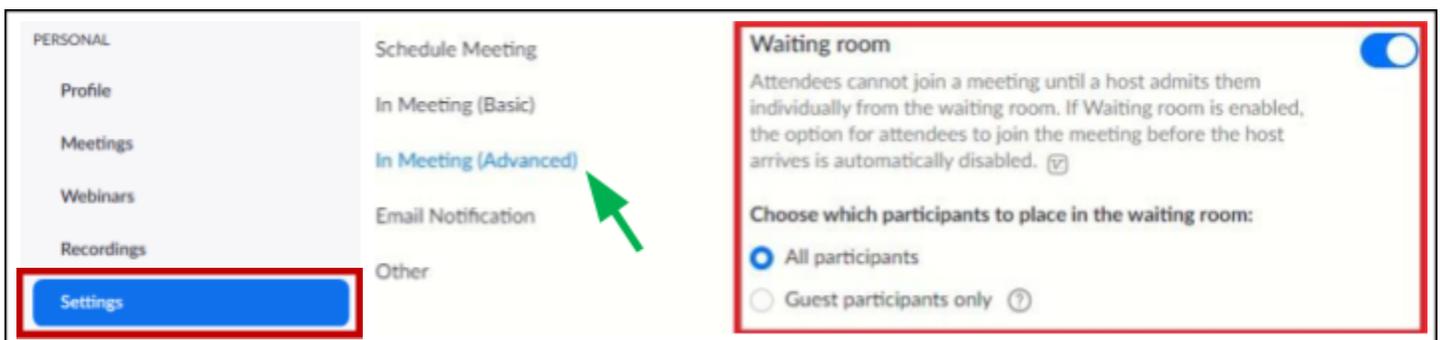
5. Only allow the meeting Host (you) to share the computer screen
This option ensures only you or a co-host can share your computer screen with the meeting attendees. You can always change this later when the meeting is in progress.

    a. Navigate to https://zoom.us/profile/setting to view your Zoom Profile settings.
    b. Select "**In Meeting (Basic)**" from the menu on the left and scroll down to **Screen sharing**. Here you can designate who can share their screen in a meeting.
    c. Click on **Host Only**. This will ensure that only the Host (you) or a designated Co-Host can share their screen during the meeting.
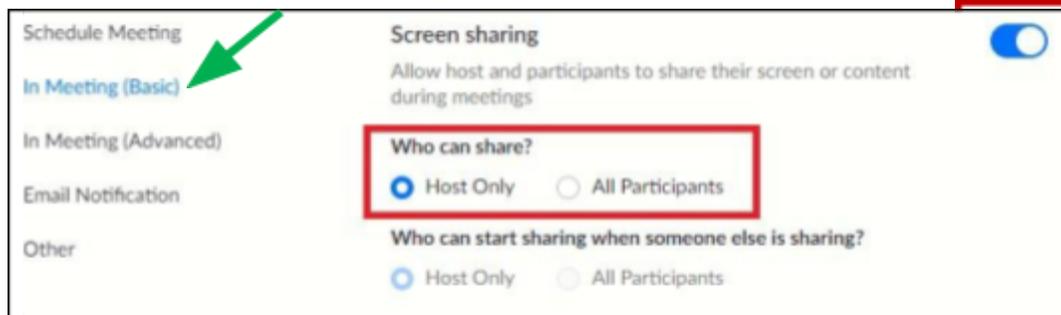
    d. If you want a trusted participant to share their screen, you can make that participant a "Co-Host" so they can share it. To make a participant a Co-Host, click on the **Manage Participants** button, hover your mouse over the participant's name, click on the **More** button, then select **Make Co-Host**.

    e. Once they are done, you can remove the Co-Host role by following the same steps and then choosing the **Withdraw Co-Host Permission** option.
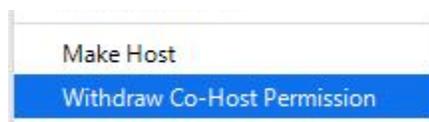
    f. If you trust the meeting participants, you can allow them to share their screens without making them a Co-Host. Click on the **up arrow** next to the Share icon (shown below), then choose **Advanced Sharing Options…**
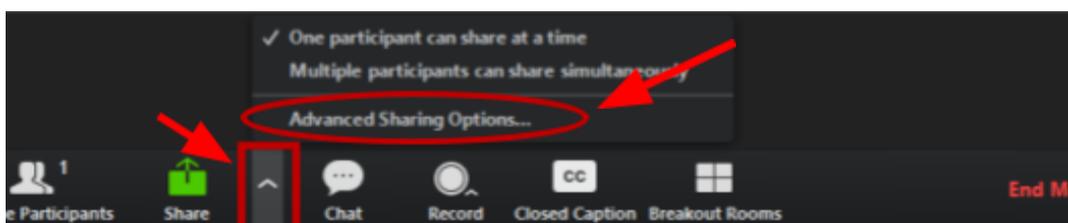

    g. Change "Who can share?" to **All Participants**. Change back to **Only Host** when you want to remove this capability from the participants.

6. **Managing Participants**
   You can **mute, unmute,** remove the **attendee waiting room** requirement, and **disconnect** (remove) participants at any time by using the **Manage Participants** list.

   a. During the meeting, click on the **Manage Participants** button. A Participants window will appear on the right side of your meeting. Click on **More** at the bottom to change the default settings for the meeting in progress.
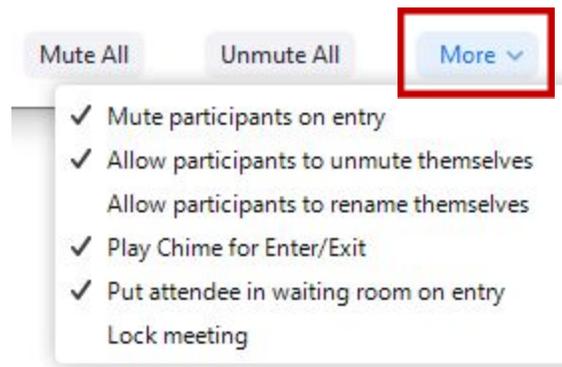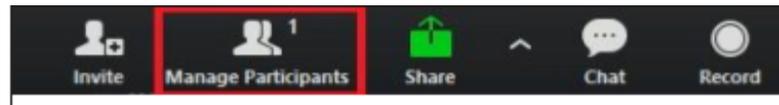
   b. **Mute participants on entry** will ensure new participants are automatically muted by default. You can prevent them from unmuting themselves by removing the checkmark next to **Allow participants to unmute themselves** (if you do this you will need to manually unmute them). If you enabled the waiting room option when creating the meeting, you can turn it off by unchecking that option here.

   c. If you choose to mute the participants by default, you can unmute them by using the **Unmute** button in the participants list by their name.

   d. You can **Mute** or **Unmute** all participants by using the buttons at the bottom of the Participants list.
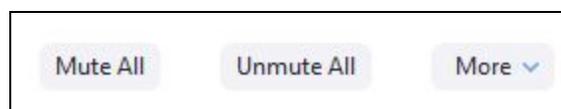
e. You can **Remove** a participant from your meeting at any time by clicking on the **More** button and select **Remove** from the list of options. Note: Once you remove a participant, they will _not_ be able to re-join your meeting.

7. **Preventing Participants from Rejoining Meetings**
   Make sure your Zoom settings are configured to prevent participants from rejoining your meetings after you have removed them from the meeting.

   a. Navigate to https://zoom.us/profile/setting to view your Zoom Profile settings.
   b. Select **In Meeting (Basic)** from the menu on the left, then scroll down to **Allow removed participants to rejoin**. Make sure this setting is _not enabled_ (see below example).
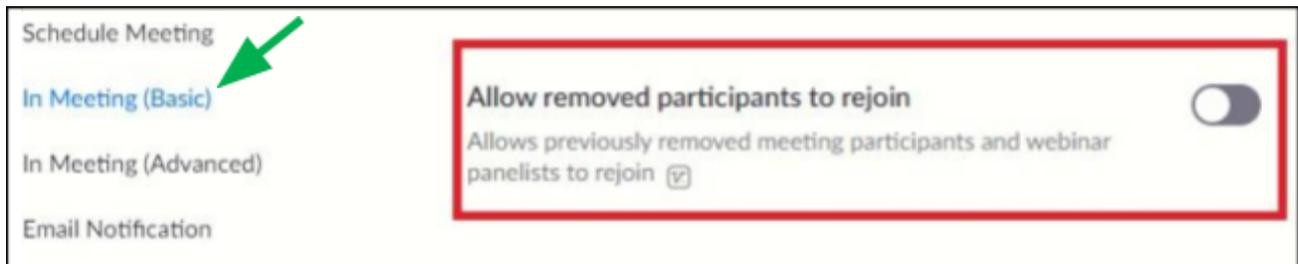
8. **Muting all participants automatically when they enter the meeting**
   You can configure your settings to mute participants automatically.

   a. Navigate to https://zoom.us/profile/setting to view your Zoom Profile settings.
   b. Select **Schedule Meeting** from the menu on the left and scroll down to Mute participants upon entry. Enable the setting (see example below).
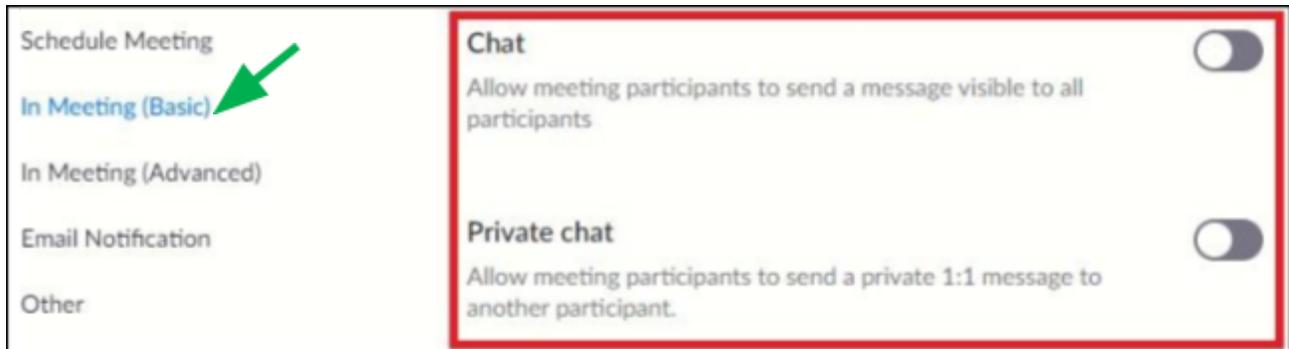
9. **Disabling Chat and Nonverbal feedback**
   If you plan to meet with students in a group setting, you may wish to disable the Chat function and "nonverbal feedback" by default. You can change this later in the meeting.

   a. Navigate to https://zoom.us/profile/setting to view your Zoom Profile settings.
   b. Select **In Meeting (Basic)** from the menu on the left. Scroll down to **Chat** and **Private chat**. This is where you can disable/enable access to chat functions (they are disabled in the below example).

   c. Scroll down to the Nonverbal feedback section and disable access to these settings.
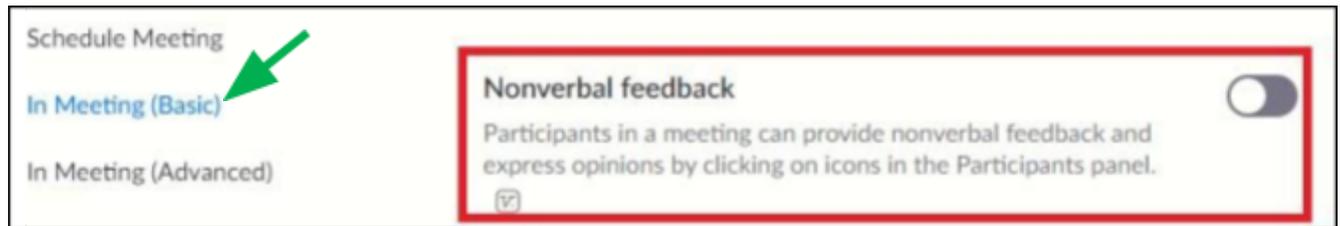
   d. You can re-enable these **Chat** features at any time in a meeting by clicking on the **Chat** button. A Chat window will appear. Towards the bottom right-hand corner of the Chat window click on the **ellipsis (…)**. Under Allow Participants to chat with: select **Host only** or **Everyone publicly** to enable the in-meeting chat. You can also elect to enable chat by default in your settings and disable it as needed.
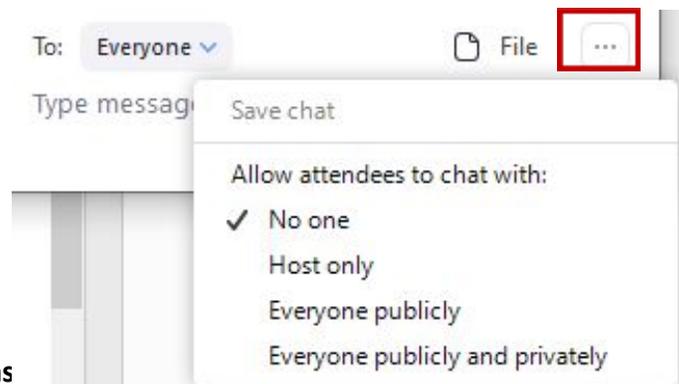

10. **Disable File Trans**
    Although it should be disabled by default, you will want to make sure **file transfers** are disabled to prevent students from sending files to each other in the **Chat** window.

a. Navigate to https://zoom.us/profile/setting to view your Zoom Profile settings.
b. Select **In Meeting (Basic)** from the left menu and scroll down to File transfer. Make sure the setting is disabled (as shown in the example below).
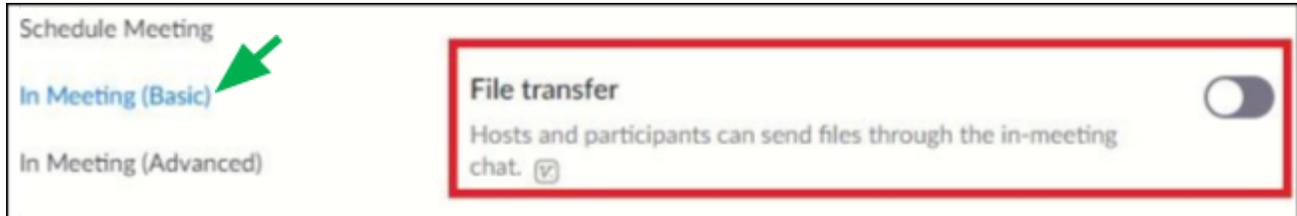

c. When disabled, users will be restricted from sending files to other participants within the Zoom meeting.

11. Locking the Meeting once all Participants Have Arrived

Once all participants have joined your meeting, you can manually "Lock" the meeting and prevent any new users from joining, even if they have the Meeting ID or weblink.

a. To Lock a Meeting, first open the Participants pane by selecting **Manage Participants** at the bottom of the Zoom Window:
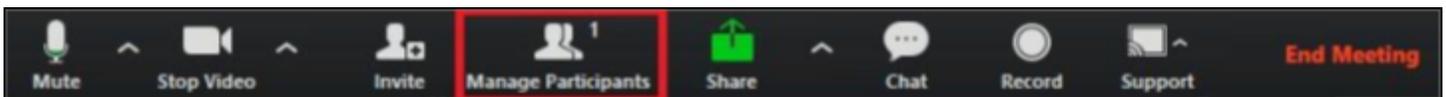
b. The Participants will typically open on the right side of the Zoom window. Select "More" from the dropdown list and then select "Lock meeting".
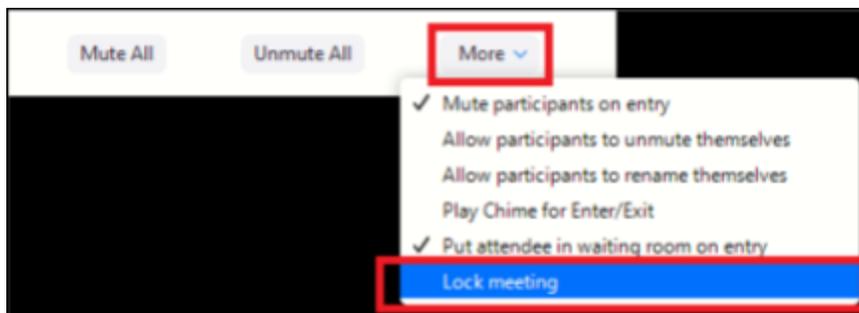
c. After you have selected "Lock Meeting" you will see a confirmation window. Click **Yes** to lock the meeting. To Unlock the meeting, remove the checkmark from the **Lock Meeting** option.

12. Hosting Public Meetings – Take Extra Precautions

Remember, any meeting that is open to the public is one that could be potentially

"Zoom Bombed" by an attendee if you don't have the meeting settings configured properly with security in mind.

Here is a list of security settings you should enable to ensure you have a successful and distraction-free meeting:

1. Only allow the Host and Co-Hosts to share their screens (never allow participants)

2. Mute all participants automatically upon entering the meeting. If needed, prevent them from unmuting themselves by clicking on **Manage Participants**, click on **More**, then remove the checkmark from **Allow Participants to unmute themselves.**

3. Utilize "waiting rooms" if you want to admit participants manually.

4. Disable the Chat and Non-verbal feedback functions. If you want to receive input from the attendees, change the Chat settings to **Host Only** to prevent them from chatting with each other or to the public.

5. Ensure the option "Allow removed participants to rejoin" is disabled in your settings. If you have an issue that requires you to **Remove** a participant, you don't want them to be able to rejoin the meeting.

6. Disable file transfers.

7. Lock the meeting once all Participants have arrived.

8. Add a Co-Host ahead of time when scheduling a meeting by entering their email address. Note that Co-Hosts must have a Zoom account in your agency's Zoom infrastructure for this to work.

9. Always be careful of where you post the meeting information. If posted on a publicly available website, be sure you tighten the security settings on your meeting as much as possible to prevent abuse.