# Securing a Zoom Meeting in Progress (and what to do if you get Zoom Bombed)

This document walks you through how to secure your Zoom meeting when it is already in progress. Be sure to also review our documents on *Setting your Zoom Security Settings Before a Meeting* and *Scheduling a Secure Zoom Meeting*.

Here's what's covered in this document (click on the menu item to advance to that section of the document):

## Contents


**Top Security Recommendations** ..... 2

**The Zoom Security Button** ..... 2

**Security Options in the Participants Menu** ..... 3

**Zoom Security Features for Individual Participants** ..... 3

**Report a Participant** ..... 5

**Zoom Security Features for Participants as a Whole** ..... 6

**Security Options in the Chat Menu** ..... 6

**Disable Participant Annotation During Screen Share** ..... 7

**Spotlight your Video** ..... 8

**What to do if you get Zoom-Bombed** ..... 8


If you have any questions after reviewing this document, or any other of our resources on the Carleton TLS - Media Production Zoom Resources page, please email us at Zoom@carleton.ca

# Top Security Recommendations

Follow these security recommendations regardless of the Zoom settings you enable or disable:

1. DON'T use your Personal Meeting ID (PMI) for public events. Your PMI is essentially one continuous meeting. Once people know the ID number, they can join the meeting at any time.

2. NEVER share your Zoom meeting links on publicly accessible forums. Instead, share link details through cuLearn so only enrolled students can access the virtual classroom.

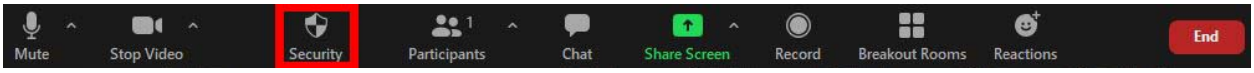
3. NEVER use the same password for your Zoom meetings, even if you are scheduling a recurring meeting for a class. You can further protect your Zoom sessions by only sharing the password shortly before a class session.

4. AVOID publicly posting images of private and virtual class meetings on social media or elsewhere online. This is important to protect the privacy of students, staff, and faculty.

5. DON'T share sensitive or confidential information on Zoom. As a standard practice, Zoom data mines all information provided on their service. There are reports that Zoom is capturing the browser 'tabs' that are open at the same time as Zoom. To avoid having Zoom gather this information, open Zoom in a private/incognito browser and avoid opening any additional tabs within that browser.

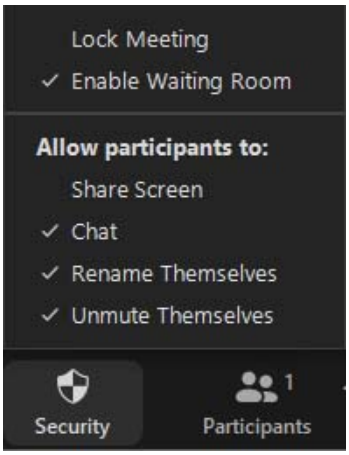
## The Zoom Security Button

Security settings are also available and accessible to you during a Zoom meeting. Some of the in-meeting security options can be found by clicking on the "Security" button in the toolbar of your Zoom meeting.




When you click on the security button, a menu will pop up that looks like this:

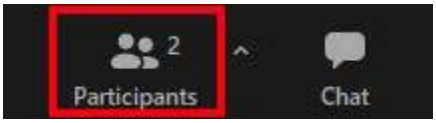
| | |
|---|---|
| Lock Meeting | Enabling this option will lock your meeting so no late or unwanted individuals can join. If you lock your meeting, know that students with internet connectivity issues may drop from the meeting and not be able to re-join unless you unlock the meeting. If you plan to use the Lock feature, establish a protocol with your class whereby they can email the host (you) if they drop out of the meeting so you know to let them back in. |
| Enable Waiting Room | You enabled this setting when you scheduled your meeting, and it is good to keep the setting enabled throughout. If any students or others attempt to join the meeting, you will be able to review who they |



| | |
|---|---|
| | are and let them into the room if you determine they are part of the class. |
| Allow participants to: Share Screen | Best to keep this feature disabled by default. You can always click on the security button and enable sharing when it is time for others to share (e.g. student presentations). |
| Allow participants to: Chat; Rename Themselves; Unmute | Best to keep these features enabled so students are able to interact with each other in the chat, and speak when called upon. Other features described below will allow you to mute everyone at once, and adjust chat functionality. |

## Security Options in the Participants Menu

Zoom also includes Security features in the participants menu. To access these settings, you must first open the participants window by clicking on the Participants button in your Zoom toolbar.

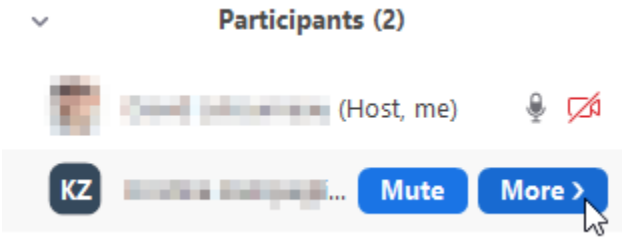



If you are using Zoom in full screen mode, the participants window will open as an extra box separate from your Zoom screen. If you are NOT in full screen mode, the participants window will open to the right of your Zoom screen. Once open, you will be able to see a list of all participants in your meeting. You will also be able to access security features for individual participants, or for participants as a group.

## Zoom Security Features for Individual Participants

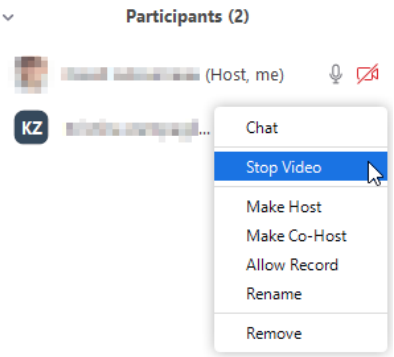
There are a few main security features you can access for individual participants: Mute, Stop Video, Remove and Put in Waiting Room. These features can be accessed as follows:

When you hover your mouse over a participant's name, two blue buttons will appear – Mute & More:



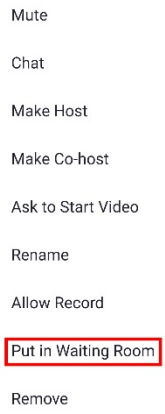

**To mute the individual**, simply click on the Mute button. If you have allowed participants to unmute their mics, the participant will still be able to unmute at will. You can disable their ability to do so by disabling the "Allow participants to: Unmute" feature found in the Security button in your Zoom toolbar (as described in the section above).

**To stop a participant's video**, click on the "More" button and select "Stop Video".




**To remove the participant** from your Zoom session, click on the "More" button and select "Remove" at the bottom of the list. If you remove a participant, they will NOT be able to re-join the meeting.

**To put an attendee on hold/Put attendee in Waiting Room**:
Attendee on hold or Put Attendee in Waiting Room allows the host to stop video and audio transmission to a participant or participants. You can do this for individual participants by clicking on the "More" button, and selecting "Put in Waiting Room".

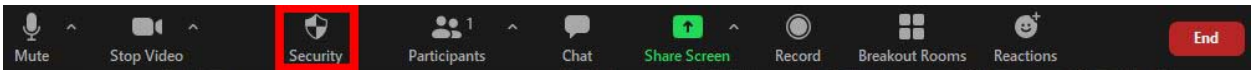



Note that you also have access to a similar participant menu by hovering over the top right-hand corner of their video stream and clicking the white ellipsis (...) that appears.

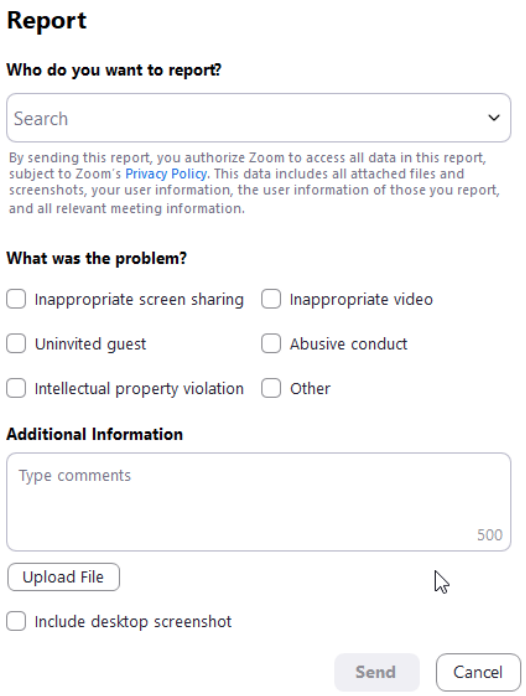
## Report a Participant

The host and/or co-host can now report a particular participant during a meeting. The meeting host/co-host will be able to select which participants they'd like to report, including any written details on why they are being reported, as well as any applicable attachments. The report will then be sent to the Zoom Trust and Safety team to evaluate any misuse of the platform and block the user if deemed necessary.

1. During your session, click the Security icon in the meeting controls bar.




2. Select Report… from the available options.
3. You will then be prompted to fill out the Report Form, where you will include the name of the participant, the problem you were facing, and any additional comments and information. You can also include attachments and a screenshot of your desktop.
4. Click Send when you have finished completing the report.

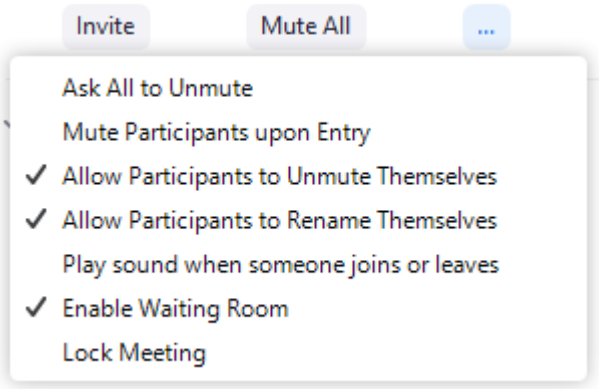


## Zoom Security Features for Participants as a Whole

Zoom also offers security features that can impact ALL the participants in your Zoom session at once. To access these features, look to the bottom of your Participants window. You will see three buttons: "Invite", "Mute All", and "…".

Mute all will mute all participants in the Zoom session. If you have allowed participants to unmute their mics, the participant will still be able to unmute at will. By clicking on the ellipses "…", you will be able to access advanced features, including disabling participants' ability to unmute themselves:

| | |
|---|---|
| Mute Participants upon Entry | It is smart to enable this feature so that participants are muted when they join the session. |
| Allow participants to unmute themselves | If you have an unwanted visitor or a rowdy participant, you can prevent ALL participants from unmuting their mics by unchecking this feature. |
| Enable Waiting room | You enabled this setting when you scheduled your meeting, and it is good to keep the setting enabled throughout. If any students or others attempt to join the meeting, you will be able to review who they are and let them into the room if you determine they are part of the class. |
| Lock meeting | Enabling this option will lock your meeting so no late or unwanted individuals can join. If you lock your meeting, know that students with internet connectivity issues may drop from the meeting and not be able to re-join. |



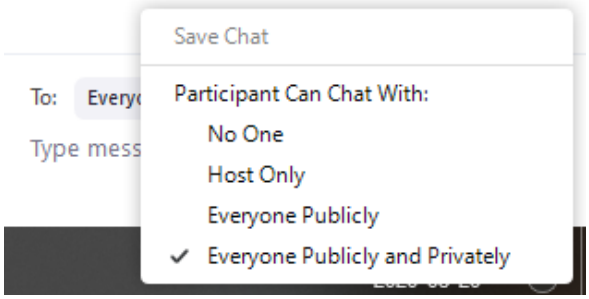

## Security Options in the Chat Menu

Zoom also offers security features in the chat menu. To access these settings, you must first open the chat window by clicking on the chat button in your Zoom toolbar.


If you are using Zoom in full screen mode, the chat window will open as an extra box separate from your Zoom screen. If you are NOT in full screen mode, the chat window will open to the right of your Zoom screen.

Once open, you will be able to access the chat security features by clicking on the ellipses ("…") button in the bottom right-hand corner of the chat box. This button will open the chat settings and will allow you to decide how participants can chat with each other and with you:

| | |
|---|---|
| No One | This option prevents participants from using the chat feature. Best NOT to disable chat entirely. |
| Host Only | This option allows participants to chat with only you. |
| Everyone Publicly | This option enables participants to chat with the group as a whole, but prevents them from sending private messages to individual participants. |
| Everyone Publicly and Privately | This is the default option which allows participants to chat with the group as a whole, as well as message individual participants. |




## Disable Participant Annotation During Screen Share

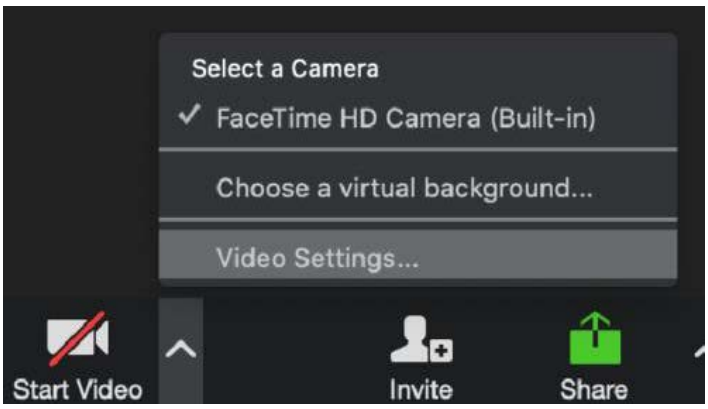
You can disable participant annotation within a meeting, for only that meeting.

1. From within your meeting, ensure you've started a share screen
2. From the Zoom tool bar located at the top of your screen, click "More".
3. From the drop-down click "Disable Attendee Annotation"

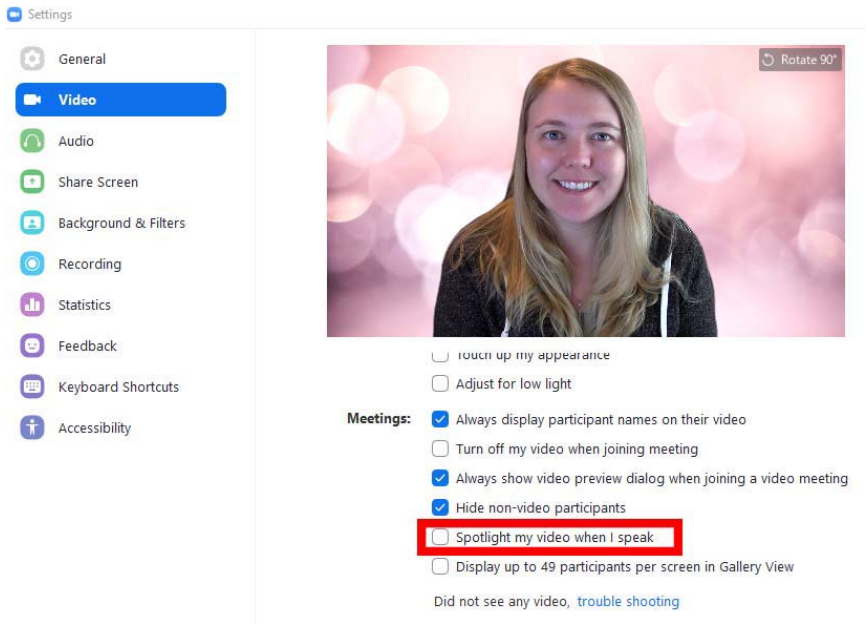
## Spotlight your Video

When three or more participants have their video turned on in a meeting, you can spotlight your video so everyone sees you as the active speaker. This can help ensure participants are focused on your video feed as opposed to that of others.

To enable the spotlight feature, click on the triangle image beside the video button in your Zoom toolbar and select “Video Settings”. This will open the video settings menu.




Scroll down the video settings menu, and place a checkmark in the box beside “Spotlight my video”.




## What to do if you get Zoom-Bombed

If you have secured your Zoom sessions to the extent possible using the features described above, your likelihood of getting Zoom bombed is VERY LOW. However, if it DOES happen, there are a few things you can do to minimize interruption and get your meeting back under control.

- Mute audio for individual attendees or everyone in the meeting, and disable the option to unmute.
- Stop a participant’s video if it’s distracting or inappropriate.
- Disable screen sharing again even if you’ve allowed participants to use this feature.
- Stop annotations so nobody can draw or write inappropriate material on shared screens.
- Disable chat or limit it to only allow participants to send messages to the host.
- Remove a participant and prevent them from being able to rejoin.
- **If the disruption is severe or harmful**, end the meeting immediately, restart, and send participants a new link and password through cuLearn.

Ultimately, the **best option** for dealing with Zoom bombing is to have a contingency plan that you share with your students through cuLearn at the start of the course. For this contingency plan, we recommend creating two meeting rooms for your classes: An “A” Room and a “B” Room. The “A” room is the main online meeting session you will use for your class. However, in the event that your “A” room gets compromised by a Zoom bomber, students will know to go to the “B” Room so you can quickly and easily resume your class.

By having an A/B contingency plan, you can avoid the fuss of attempting to evict a Zoom bomber and can instead focus on a quick transition to the new online space.

Be sure to also review our documents on *Setting your Zoom Security Settings Before a Meeting* and *Scheduling a Secure Zoom Meeting* in order to run the most secure Zoom sessions possible.