

Safety Checklist for ZOOM Hosts:

Generic Zoom suggestions to be aware of - Before Meeting:

- Disable autosaving chats
- Disable file transfer
- Disable screen sharing for non-hosts
- Disable remote control
- Disable annotations
- Use per-meeting ID, not personal ID
- Disable “Join Before Host” (*disadvantage to this is you as a HOST have to be there so use with caution*)

During Meeting:

- Assign at least two **co-hosts** –
The Meeting Participants icon when pressed – brings a column over to the right and allows control over most aspects of the participants
- **Mute** all participants and explain how they can unmute themselves – the co-hosts also have the ability if a new user doesn’t know how yet
- Have people use **headphones** if there are other people in the home (protects the privacy and anonymity of the attendees)
- Anonymity: **Screen Name** – invite people to change their own Display Name or as a Co-Host scroll over their screen – press the three dots and keep their last initial/remove their last name.

If you are Zoombombed:

- Remove problematic users and disable their ability to rejoin when asked
- Lock the meeting to prevent additional Zoombombing – *again use with caution as this will not allow new attendees to log in*

Instructions for HOSTS in how to perform all of these steps are included below:

While most meetings won't be Zoombombed, there are some safety measures that you can take when you host a Zoom meeting. ADL's Center for Technology and Society recommends the following:

When scheduling or setting up a meeting you will host:

Set Safe Meeting Default Settings

On the Zoom Settings page, turn off participant controls:

- 1) Sign into Zoom.us.
- 2) Click on the Settings link on the upper right (it looks like a gear).
- 3) On the right side of the page, turn off: Autosaving chats, file transfer, screen sharing, and remote control.

Assign a Co-Host

For larger meetings, identify a co-host or two ahead of time whose role is to be a virtual room monitor and manage order during the meeting by managing the participants. Co-hosts are assigned during a meeting and cannot start a meeting.

- 1) Sign into Zoom.us.
- 2) Click on the Settings link on the left of the screen.
- 3) Scroll down to the Co-host option on the Meeting tab and verify that the setting is enabled.
- 4) Turn on Co-Host. If a verification dialog displays, choose Turn On to verify the change.

Assign a per-meeting ID, don't use your Personal Meeting ID

Avoid using your Personal Meeting ID (PMI) to host public events. Your PMI is basically one continuous meeting - your personal virtual space; and once it is published, others can join at any time. Learn about meeting IDs and how to generate a random meeting ID (at the 0:27 mark) in this video tutorial.

Prevent Screen Sharing by non-hosts

To prevent participants from screen sharing during a call, use the host controls at the bottom of the window, click the arrow next to Share Screen and then choose Advanced Sharing Options.

- Under “Who can share?” choose “Only Host” and close the window. You can also lock the Screen Share by default for all of your meetings in your web settings.

Disable Join Before Host

Before starting a meeting, disable Join Before Host to keep users out before the host arrives. This is the current default, but double check to make sure that it is set for the meeting. When “Join Before Host” is enabled, anyone can enter at any time and create havoc with other participants before the meeting officially starts.

Turn off file transfer

In-meeting file transfer allows people to share files through the in-meeting chat. Toggle this off to keep the chat from getting bombarded with unsolicited pics, GIFs, memes, and other content.

Turn off annotation

You and your attendees can doodle and mark up content together using annotations during screen share. Disable the annotation feature in your Zoom settings to prevent people from writing all over the screens.