

Zoom Security Essentials
For OA- Orange County Intergroup
Including a step-by-step guide to deal with Zoom bombing
V. 2.0 – 11/21/20

This sheet summarizes measures to prevent and deal with Zoom disruptors.

Please report any disruptive incidents to me, describing how the disruption was done and what you did about it, and how people are feeling. We are all learning! Feel free to call me (Terry) at 949-400-3379.

MOST IMPORTANT!

1. **The meeting settings in the Zoom account should be set to ‘Share Screen’ for Host only.** Make sure this is set in the meeting settings so it comes up automatically any time the meeting is started.

With this setting, the Host can make anyone who needs to share screen a Co-Host. This prevents disruptors from displaying graphic images that can be highly disturbing. People wanting to share screen can be made Co-Hosts. Hosts and Co-Hosts can check this setting under the security shield icon—“Participants can...Share Screen” should NOT be checked.

NEXT MOST IMPORTANT...

2. **ALWAYS have a Host AND Co-Host (s)** during every meeting.

Why? Because only Host and Co-Host can use security features.

Why have a Co-Host too? Zoom-bombers usually travel in threes. Three is too many for one person to handle.

How do I make someone Co-Host? Only the Host can make someone Co-Host. Choose the person in the Participants window, click on “...” or “More” and choose “Make Co-Host.” Please volunteer to be a Co-Host if you are willing and able.

3. Never publish a one-click Zoom link on the web or Facebook.

4. **Should a disruption occur, Host or Co-host must act immediately:**

(Directions apply to computers; iPads have different menus)

- A. **Take a deep breath.** Announce that the meeting is being Zoom-bombed, and that you are dealing with it, and that people may wish to turn off sound and step away from their computer for a minute.
- B. **Mute all** (button at the bottom of the Participants window)
- C. **Uncheck “Allow Participants to unmute themselves”** (in More or “...” menu, bottom right of participants window.
- D. **Disable Participants Chat** (“Participants can chat with... No One”, found in “...” or “More” menu at bottom right of chat window)

- E. **Identify likely troublemakers and “Put in Waiting Room”** (in More or “...” menu for the participant, either in their video tile or to the right of their name in the Participants window. (You do NOT need to “Enable Waiting Room” to do this.)
- F. **Take another deep breath.** Your meeting is safe. Undo steps B, C & D.
- G. **Sort out the waiting room.**
 - a. “Remove” any obvious malicious persons from the waiting room. They will not be allowed into that day’s meeting again.
 - b. “Admit” any members known to you.
 - c. Send a message to any remaining people in the Waiting Room, asking them to call or text someone (who is willing) telling them what meeting they’re here for.
- H. **Check in with meeting participants.** How are they feeling? Do they need a little meditation or the serenity prayer? Does anybody need some one-on-one support?

Please let me know if you want a quick training/review about meeting settings and how to respond quickly and appropriately to any disruption.

Here are more secure options that are less friendly to the newcomer, that your meetings’ Group Conscience may choose.

The Host or Co-host can choose to "enable waiting room" in the menu under the security shield or in the account meeting settings. If you have Waiting Room enabled during the entire meeting, a host or co-host will need to monitor the Waiting Room, to let people in if they show up. You can chat to the waiting room, asking them to phone or text what meeting they want to attend. Please be courteous: 99% of unknown people will be newcomers, not troublemakers. You can use a phone/text app like Google Voice if you do not want to give out a regular phone number.

If your meeting’s group conscience does not want to deal with behavior of this type ever, you can remove your meeting’s Zoom passcode from the web page. People wishing to attend would need to call the contact listed on the Web to get the passcode. This is great for security and not great for our 12th tradition of reaching out. It is analogous to a meeting being held in a gated community and phoning for the gate code. Let me know if your meeting wants to make that change.

Thank you for letting me be of service, and I hope we all stay secure and serene.

Terry L
E-Media Manager
emediamgr@oaoci.org