Videoconference Meeting Training and Security/Preventive Measures

Region 8 created this document to address disrupters/intruders at OA meetings. This document is adapted from the OA World Service information sheet on the same topic and references the Zoom videoconferencing platform and Zoom-specific functions. This is not an endorsement of the Zoom platform, only a reference tool.

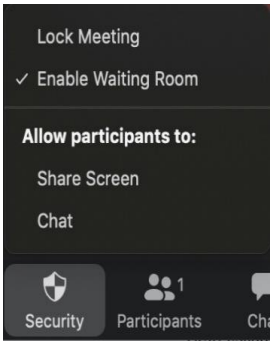
General Information

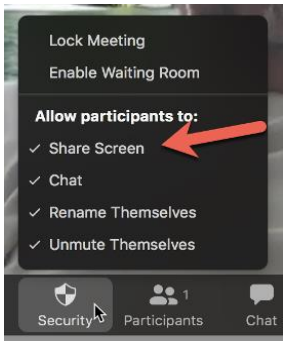
It is important that OA members are trained and familiar with using a videoconference platform.
You may want to pre-assign these positions for each meeting. It is recommended the account be set to have a two-factor authentication. Limit who has the account login information. Limit who has the host code to those who regularly attend the meeting. Recommend guidelines that members to not record or screen capture meetings to protect anonymity. It is not against our traditions to remove intruders. Intruders detract from our ability to carry the message and detract from the common welfare of OA as a whole.

Optional Security Measures

Waiting room- As participants log in to your meeting, they are placed in a waiting room, and the host/cohost grants permission to enter the meeting. This is a security setting that can be set up in advance when you schedule your meeting or it can be turned on during your meeting at any time. If this is set in advance, no one can enter the meeting and the meeting can only be started by someone signing into the Zoom account and starting it from there, which will automatically make they host. It is not recommended that the login credentials be shared freely. And with two-factor authentication, the person logging in the meeting will not get the email for authenticating. I think this should be changed so it only indicated the host log into the meeting and claim host. And they should log in at least 15 minutes before start of meeting to put on waiting room.

Video option- You may enable and disable the video-viewing setting of each meeting participant or all participants.
Chat option- Allows host to set so OA members may chat only with the host or with everyone.
Muting –Zoom allows OA members to mute and unmute themselves unless the host disables that setting. Once the setting is disabled, only the host can request the attendee unmute themself. Recommended for meetings where not all the attendees are regular members or for larger meetings.
There may be other functions within the videoconferencing platform that need to be enabled or disabled. Check for updates to your videoconferencing platform, and check the settings after an update has been completed.



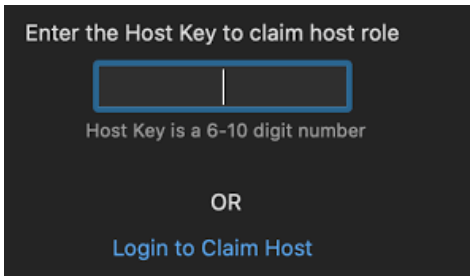


Recommended Videoconferencing Service Positions

Host

Signs on fifteen minutes before the meeting starts and enables waiting room. If the waiting room is enabled, then OA members cannot access the meeting until the host/cohost grants entry. Claims host setting. Enables

waiting room. Makes assigned members cohosts. Confirms screen-sharing function is disabled for attendees. Confirms if disrupter/intruder is present and remove the intruder or use of Security Shield to suspend participant activities.



Cohost
Your meeting may choose to disable participants' ability to unmute themselves. This is recommended for larger meetings. A cohost will need to choose participant with electronically raised hand to share. (Participant must raise hand electronically to be recognized.) Asks participant to unmute, allows hand to stay raised until member finishes speaking. Leaving the hand raised keeps the person's video to be highlighted. Cohost then mutes participant and lowers hand when member finishes speaking. Meeting intruders may work together and notify each other there is an "open mike" meeting where people may unmute themselves.

Security Monitor
Shares format or literature on-screen, only sharing OA or AA copyrighted readings. (See the Sharing OA-Copyright Material Electronically letter at oa.org/document-library) Turns off video, if needed. Works with others to confirm if disrupter/intruder is present and remove the intruder or use of Security Shield to Suspend Participant Activities.

Chat Monitor
Monitors the chat; if problems arise, contacts Security Monitor to remove persons disturbing the chat. Shares meeting items to place in the chat.

Timekeeper
Times member shares and gives a reminder and time left when member's time is concluding.

Security and Preventive Measures

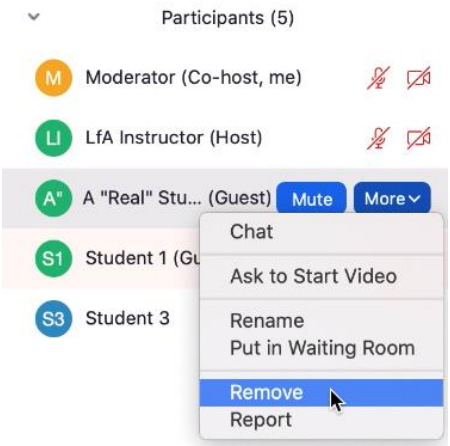
It is important to have a plan in place for addressing those who want to disrupt your meeting. It is not recommended you start a meeting without a host and others assigned to service positions. Make sure screen sharing, whiteboards and collaborating with Zoom apps are disabled for attendees. Disable the video function to ensure backgrounds and profile photos don't show inappropriate graphics. Watch for those entering the meeting after it has started.

"**Deep Fakes"** Intruders are using new tactics to disrupt meetings. They are using fake sign ins using a regular member's still image, listed phone number or "deep fakes" to get control of a meeting. A "deep fake" is a computerized moving video mimicking a person. It is recommended to ask other members personal information or a predetermined verbal password (set outside the meeting) to confirm their identity before making this participant a cohost. Once an intruder is a cohost they can not be removed from the meeting. Intruders may also say or name themselves in a way as though they are a "Zoom Administrator" or employee. Zoom staff will not ask you to share host passcodes or make them a host.

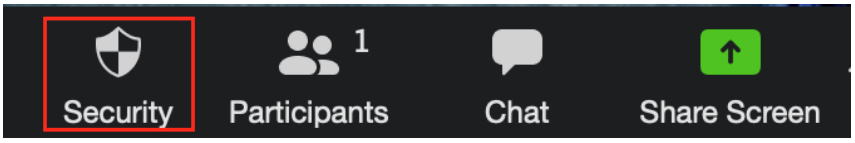
Meeting Disruption

If an intruder gains entry to your meeting and begins disrupting the meeting, there are options: remove the

intruder or use Security Shield. Intruders may be removed from a meeting by host/cohost going to the participant's box, hovering over the name of the intruder, and selecting "Remove." In Zoom settings disable the setting to "allow removed participants to rejoin". Using the same process, you may also choose to move a potential intruder into the waiting room and then chat with the person to determine if they are an intruder by asking them questions.



A different option than removing the intruder is using Security Shield. Click on "Security Shield," (green shield with check mark), and select "Suspend Participant Activities." This shuts down all of the meeting's activities. Pause for a few moments. Scan the screen for suspicious participants. Enable chat (under the Security Shield) and type a short explanation of the pause to members. Monitor the chat for intruders. Look for insults or slurs. When you are confident, you can enable participant activities and resume your meeting. Consider saying the Serenity Prayer.



We are all here to carry the message of recovery through the Twelve Steps to the still-suffering compulsive eater. It is importance to encouraged members to learn basic Zoom security skills to assist the meeting. Remember, the perceived intruder or disrupter may be a newcomer, member, or returning member unfamiliar with videoconferencing or in the middle of their disease. Patience is encouraged. Together we can do what we could never do alone.

OVEREATERS ANONYMOUS®
Region 8