Videoconference Meeting Training and Security/Preventive Measures

Purpose

In November 2021, the Board of Trustees created the Zoom Bombing Ad Hoc Committee to address growing concerns about disrupters/intruders at OA meetings. This document was created by the ad hoc committee and references the Zoom videoconferencing platform and Zoom-specific functions. These suggestions may provide guidance on using other video-conferencing platforms as well. This is not an endorsement of the Zoom platform, only a reference tool.

Training

It is important that OA members who are leading videoconference meetings are trained and familiar with using a videoconference platform.

Step 1: Determining the best videoconferencing platform for your online meeting

- Does your meeting require a waiting room? The Zoom platform allows you to enable the Waiting
  Room feature. As participants log in to your meeting, they are placed in a waiting room, and the host or cohost grants permission to enter the meeting.
- Does your meeting require a video option? The Zoom platform allows you to enable and disable the video-viewing setting of each meeting participant. The host can disable the video-viewing setting so no attendee can turn their video on.
- Does your meeting require a chat option? The Zoom platform allows you to enable the chat function to allow OA members to chat with the host only or with everyone attending the meeting.
- Do you want to allow meeting participants to mute and unmute themselves? The Zoom platform allows OA members to mute and unmute themselves unless the host disables that setting. Once the setting is disabled, only the host can unmute attendees.

There may be other functions within the videoconferencing platform that need to be enabled or disabled. It is recommended that you review all settings and determine what is best for your meeting.

Always check for updates to your videoconferencing platform, and check the settings after an update has been completed.

Step 2: Determining videoconferencing service positions

Below are recommended service positions that can help your meeting move smoothly so that the meeting's focus is on carrying the message to all compulsive eaters.

- Host
  - Signs on ten minutes before the meeting starts
  - Claims host setting
  - Enables waiting room
  - Makes assigned members cohosts
  - Confirms screen-sharing function is disabled for attendees
  - Disables participants' ability to unmute after the Serenity Prayer (beginning of meeting)
  - Enables participants' ability to unmute before the Serenity Prayer (end of meeting)

- Cohost
  - Chooses participant with raised hand to share. (Participant must raise hand to be recognized.)
  - Unmutes participant, allowing hand to stay raised until member finishes speaking
  - Mutes participant and lowers hand when member finishes speaking

- Video Monitor
  - Shares literature on-screen, except OA or AA readings, and places relevant format sections in chat. See the Sharing OA-Copyright Material Electronically letter at oa.org/document-library.
  - Turns off video, if needed
  - Works with other monitors to confirm if disrupter/intruder is present and whether the use of Security Shield to Suspend Participant Activities is necessary

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

- Security Monitor
  - Changes settings by muting all upon entry so that participants can't unmute themselves
  - Renames members according to the meeting's required naming convention, if applicable
  - Works with other monitors to confirm that a disrupter/intruder is in the meeting and whether the use of Security Shield to Suspend Participant Activities is necessary

- Timekeeper
  - Times member shares and gives five-minute, one-minute, and time notices when member's time is concluding

It is important that those selected for these service positions are trained on the videoconference platform. You may also want to create a weekly schedule and pre-assign these positions for each meeting.

Security and Preventive Measures

It is important to have a plan in place for addressing those who want to detract from the meeting or who disrupt your meeting.

Step 1: Determining security settings

- If your videoconferencing platform, such as Zoom, allows for a waiting room, it is recommended that you enable that feature. This allows the host/cohost to grant entry on an individual basis. If the host/cohost does not recognize the OA member's name, they may want to ask them why they are attending the meeting.
- For larger meetings, it is recommended that you disable participants' mute/unmute setting so that the host/cohost can determine who is next on the list to share and can unmute them when it is their turn. Smaller meetings may not need to use this function.
- If video is not necessary, you may be able to disable this function, and members can simply listen to the shares during the meeting.
- If the chat function is available, such as with Zoom, it is recommended that you set that to host only. Allowing all attendees to chat with everyone can be distracting during the meeting and may detract from members' shares.

Step 2: Preventive measures

- It is recommended that the host always arrive about ten minutes prior to the opening of the meeting. If the waiting room is enabled, then OA members cannot access the meeting until the host/cohost grants entry. Arriving early allows the host to set up the meeting's security if it is not already set.
- Ask the other service position members to arrive early so you can enable cohost responsibilities and they can prepare to fulfill their assigned duties.
- You should never start a meeting without a host and others assigned to service positions.
- Make sure screen sharing is disabled for attendees. It can also be helpful to 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. They may be an OA member who is running late, but they could be an intruder who is there to disrupt your meeting.

Meeting Disruption

If an intruder gains entry to your meeting and begins disrupting the meeting, there are several steps you can take to remove this person or place them in the waiting room. The information below is specific to the Zoom platform and is used as an example. It is recommended that you research the tools available on the videoconferencing platform you are using for addressing disruptions to your meeting.

- Click on "Security Shield," located in the top left corner of your screen (green shield with check mark) and select "Suspend Participant Activities." This shuts down all of the meeting's activities.
- Pause for a few moments and watch for attendee numbers to decrease as the intruder(s) leave the meeting.
- Scan the screen for suspicious participants and private message the cohost with name(s) to monitor.
- Enable chat (under the Security Shield) and type a short greeting to members.
- Monitor the chat to see if any intruders are still in attendance. Look for insults or slurs.
- When you are confident, you can enable participant activities and resume your meeting. Consider saying the Serenity Prayer, if needed.

Intruders can be removed from a meeting by going to the participant's box, hovering over the name of the intruder, and selecting "Remove." In Zoom, there is a setting to "allow removed participants to rejoin." If this is disabled, when someone is removed from a meeting, they cannot regain access. 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.

Deepfake Intrusions

Recently, disruptions have occurred by suspects who are using deepfake technology to mimic a real person who is a regular member of the group. The mimic pretends to attend the meeting, just as the regular member does. There was an incident where a videoconference host was tricked into giving the Zoom host codes to another attendee who they thought was the real meeting host.

We appreciate the regions for their quick response and assistance with this problem.

Given that we WILL see more clever tricks from bad actors who want to disrupt our meetings on Zoom and other videoconference platforms, we have provided additional tips to help you reduce the risk of disruptions by intruders, as well as deepfake intrusions.

Additional recommendations

- Verify that you are using the most updated version of Zoom with access to the latest security measures. Remember, never start a meeting without a host.

- If you feel your host code has been compromised, then immediately change it.
- Protect host codes as sensitive information. Set parameters as to who can access them.
- Establish a code word with your host and alternative hosts.
    - Set up a code word with all your hosts that only the hosts know.
    - Do not write this code word down.
    - Since a deepfake attendee may look like one of your meeting's members, ask for the code word when you are asked for the host code (only on camera or phone).
    - If you don't have a code word set up, before transferring the host code during the meeting, ask the person to whom you are giving the code to turn on their video. Have a conversation with this person, asking questions that require more than a yes or no answer.
    - If possible, ask personal questions that only that person would know or for information not readily available on the internet. Verify that the answers are correct, and that the person seems "right."
    - Then you will be able to send the correct person to the waiting room and do so.

We are all here to carry the message of recovery through the Twelve Steps to the still-suffering compulsive eater. 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.

OA Board-approved

Overeaters Anonymous®, Inc.
6075 Zenith Court NE
Rio Rancho, New Mexico 87144-6424 USA
PO Box 44727, Rio Rancho, NM 87174-4727 USA
1-505-891-2664 • info@oa.org • oa.org