MONTEREY BAY ACA INTERGROUP MEETING DRAFT AGENDA

Saturday, May 27, 2023, 4-5:30 PM

Meeting by Zoom ID: 898 9797 7526 PW: 792214

https://us02web.zoom.us/j/89897977526?pwd=eUx1RzRnS003QThzQ2hwblA1RUZsQT09

ACA Serenity Prayer

Request volunteer / volunteers to protect and lock down the meeting from zoom bombers, if needed.

Mission Statement and Commitment to Service of Monterey Bay ACA Intergroup

5th Tradition and 5th Concept

Guidelines for Business Meetings

Welcome to all the IGReps.

Vice Chair recognizes any new IG Reps, proxies and visitors. Determine who is eligible to vote

MINUTES – Approval of April 22, 2023, meeting minutes

REPORTS

- **Chairperson (Paul & Evie)**

- **Vice Chairperson (Renee)**

- **Secretary (Jeannie)**

- T**reasurer (Dottie)**

- **WSO Representative (Peg)**

InterGroup Rep. REPORTS

COMMITTEE REPORTS

- Literature Committee (Carol)

- Website Committee (Evie)

- Virtual Speaker Meeting Committee (Shari)

- Workshop Coordinator (Open Position)

- Outreach Committee (Rosa)

OLD BUSINESS –

Results so far - Workshop poll from members, report from Carol

Zoom "bombing" protocol for this meeting and as a template for other ACA meetings. Here is the link to an existing protocol that was submitted to the IG for consideration at April's meeting. (Text is included at REFERENCE DOCUMENTS at end of agenda.) Follow up to decide whether to recommend to area meetings for use in securing their meetings.

[Preventing and Responding to Zoombombing | Brightspace | Vanderbilt University](#)

NEW BUSINESS –

Intergroup Open house six year anniversary - possible committee formation

Is there anyone willing to volunteer as workshop coordinator for the remainder of 2023?

(if no volunteers) Solicitation of volunteers for managing a single workshop (from survey results)

—----------------------------

Evaluations

Acknowledgements

Motion to Adjourn

Referenced Documents:

Workshop Coordinator Position Summary January 2021
(amended)

This position would include:
- Be the point person for the google email account and manage the Google Drive.
- Polling our fellowship to find what the interest is in workshops (some suggestions are already formed, then prioritizing them and presenting to Intergroup).
- Research suggestions for additional relevant workshop topics and facilitators from other ACA IGs and beyond.
- Create and maintain a workshop calendar and post announcements.
- Create flyers (with help from others) and email flyers to acamontereybay@gmail.com to be distributed to the fellowship.
- Coordinate Zoom support for workshops.
- Oversee workshop presentation process.
- Offer Workshop Facilitator support.
- Navigating and facilitating the transition from Zoom only workshops to the presentation format that will prevail following the cessation of pandemic protocols.
- Assist in the fine tuning and the ongoing tasks of this newly created position.

Preventing and Responding to Zoombombing

With the exponential growth in the use of video conferencing tools around the world, Zoom in particular has suffered from a destructive trend called Zoombombing. In this guide, we'll explore what Zoombombing is and how to deter potential Zoombombers with easy-to-use security features (like enabling the waiting room or locking your meeting). We'll also look at the question of how to respond if your class is targeted by Zoombombers.

What is Zoombombing?

Zoombombing is when uninvited participants join an in-session video conference and make themselves known, often in offensive or disturbing ways. A large percentage of Zoombombing cases seem to happen in one of two ways.

1. Sometimes students in the course share class meeting information with or without the intention of inviting Zoombombers.
2. Zoombombers can also pick meetings to attend, either by choosing publicly-posted meetings or choosing random meeting IDs to join.

There is a slim chance that you will be directly affected by Zoombombing. The likelihood goes up if you post your meeting link publicly or fail to use available security features. Because the incidents tend to involved hateful, hurtful, or offensive images and speech, the effects of Zoombombing are large enough to warrant preventative measures, no matter how small the likelihood that you will be affected.

The best way to prevent Zoombombing is to avoid sharing your meeting links publicly. **If you must share a meeting link publicly, use preventative measures (e.g. enable security features like the waiting room) and have one co-host or alternative host ready at all times to respond (e.g. remove uninvited participants using the "Manage Participants" tool).** Keep reading for more guidelines for using Zoom security features to prevent and respond to Zoombombings.

How can you prevent Zoombombing?

Knowing that Zoombombing is a small but real possibility will help you prepare ahead of time to manage difficult circumstances when they arise. Start by getting to know your Zoom meeting settings and interface. Setting aside 20-30 minutes to explore your options on Zoom as you

read through this guide will greatly improve your facility with Zoom controls. You can explore either alone or with a colleague who also wants to learn more, and we highly recommend using [our Zoom guides](#) and [Zoom's privacy and security guides](#) as a starting place.

Vanderbilt Default Settings

At Vanderbilt, we have some default settings in place to protect users against these kinds of attacks. All of the measures described below can also be changed by meeting hosts. So, if you find you need to open your meeting up to allow participants more leeway, that is also possible.

- **Only host can annotate**. For meetings hosted by Vanderbilt users, the annotation tool is only available to the meeting host. This prevents uninvited guests from using the tool to interrupt your meeting. If you want your students to use the annotation tool, you will need to change this setting before the meetings starts.
- **Meetings password protected.** All meetings created by Vanderbilt users will require a password unless the host specifically disables this setting when creating the meeting. Students logging on through Brightspace or using the link for the meeting will not need to enter the password in order to join the meeting. However, any participant who uses the Meeting ID to join the meeting can only join if they also have the password. This will prevent random Zoombombers from stumbling across your meeting.

Optional Tools Users Can Enable

In addition to the above default settings, you have other Meeting Options available to add more security.

- **Enable waiting room**. If you turn this setting on, students will start in the waiting room and you or another host will have to manually admit each student into the class meeting. If uninvited guests show up, you can simply NOT admit them.

- **Authenticated users only**. If you click on this option, only Zoom users who have signed in to their accounts can get into the Zoom meeting. This will make it harder for anonymous participants to bomb your meeting, and easier to track anyone who does arrive uninvited.
- **Lock the meeting.** Once a meeting begins and all attendees are in the meeting, one of the most effective ways to deter Zoombombing is by **locking the meeting**. Much like locking the door of your classroom so no one else can enter, locking your meeting does not allow any more participants to join whether or not they have the password. First click on the Manage Participants button at the bottom of your screen. Then, choose the More option, and finally, click Lock Meeting.
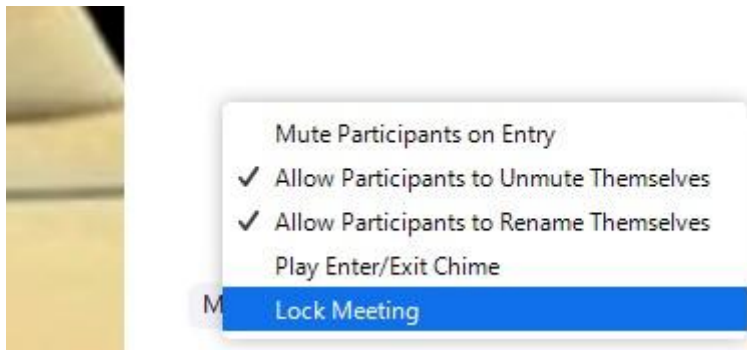
In recent weeks there have been many useful posts and essays on the web about how to prevent Zoombombing.

- [How do I deter Zoom bombers?](#) This guide was created by [Michelle Pacansky-Brock](#) and shared with a creative commons license, March 2020
- This blog post from Zoom called [Best Practices for Securing Your Virtual Classroom](#)
- This post from the ADL has [extensive instructions on how to completely lock down your Zoom meeting](#), even if you are hosting a publicly accessible event.

How should you respond if your class is targeted by Zoombombers?

If you find, despite your precautions, that Zombombers have found their way into your classroom, you also have options for dealing with the crashers once the meeting has started.

- **Remove a participant**. If you realize that someone has become disruptive, you can always turn off that participant's audio and/or video or just remove them from the meeting entirely using [these instructions](#).
- **Lock the meeting behind removed participants.** After you have removed the uninvited guest, lock the meeting behind them (see instructions above).

- **Mute all audio** if the uninvited guests are being disruptive through audio. You can use the keyboard shortcut **Alt+M**: Mute/unmute audio for everyone except host.
- **End the meeting for all participants**, and then restart the meeting using the Waiting Room setting. This will allow you to quickly eliminate the disruptors, and then one-by-one allow legitimate participants back into the meeting in order to resume business with minimal damage done.
- **Report.** If your class is targeted by Zoombombers, please reach out to Brightspace support at brightspace@vanderbilt.edu to report the incident. We will immediately loop in appropriate staff and admins to investigate your meeting records and seek out the identity of the bomber.

Use the privacy and security measures that will work for your course, and learn the tools for silencing or removing participants during a meeting. These steps will go a long way towards securing your classroom against Zoombombing and giving you peace of mind as you teach.