Navigating Virtual Hate

Adapted from a presentation by Sumun L. Pendakur and Jade Agua, USC Equity Center
Some language has been altered to make it more applicable to audiences beyond colleges (e.g., replacing "students" with "participants")

What is "ZoomBombing"/ "ZoomTrolling"?

- This is a form of cyber attack
- It is intended to be disruptive and create harm through written words, images, or invectives that are racist, sexist, anti-Semitic, transphobic, and so forth
- It is not simply "party crashing" – calling it such diminishes the impact of these attacks
- Related to broader patterns of white supremacy, xenophobia, misogyny, heterosexism, cissexism, and so on.
    - Increased surge of overt and violent attacks IRL (In Real Life)
    - ZoomBombing/ZoomTrolling has also occurred in virtual town halls in response to IRL attacks
    - This has a particularly damaging ripple effect for the most marginalized amongst us and is used as a silencing mechanism

Q: Have you or someone you personally know experienced ZoomBombing/ZoomTrolling?
Of the 258 attendees of the session who responded, 45% said yes, they had.

Consider other options

- Zoom Webinar
- Google Hangout (free for up to 10 people meetings)
- Google Meet
- WebEx
- Ring Central
- Microsoft Teams
- GoToMeeting ($12/month for up to 150 people)
- Jitsi Meet (free and no account necessary, for inviting people into meetings at the time of the meeting, i.e., unable to schedule and create a link ahead of time)
- Whereby (for small group meetings, free for personal use)
- Skype for Business

See this article for more information about security and privacy on some of these other options.

What to do when planning, scheduling, and running a meeting on Zoom

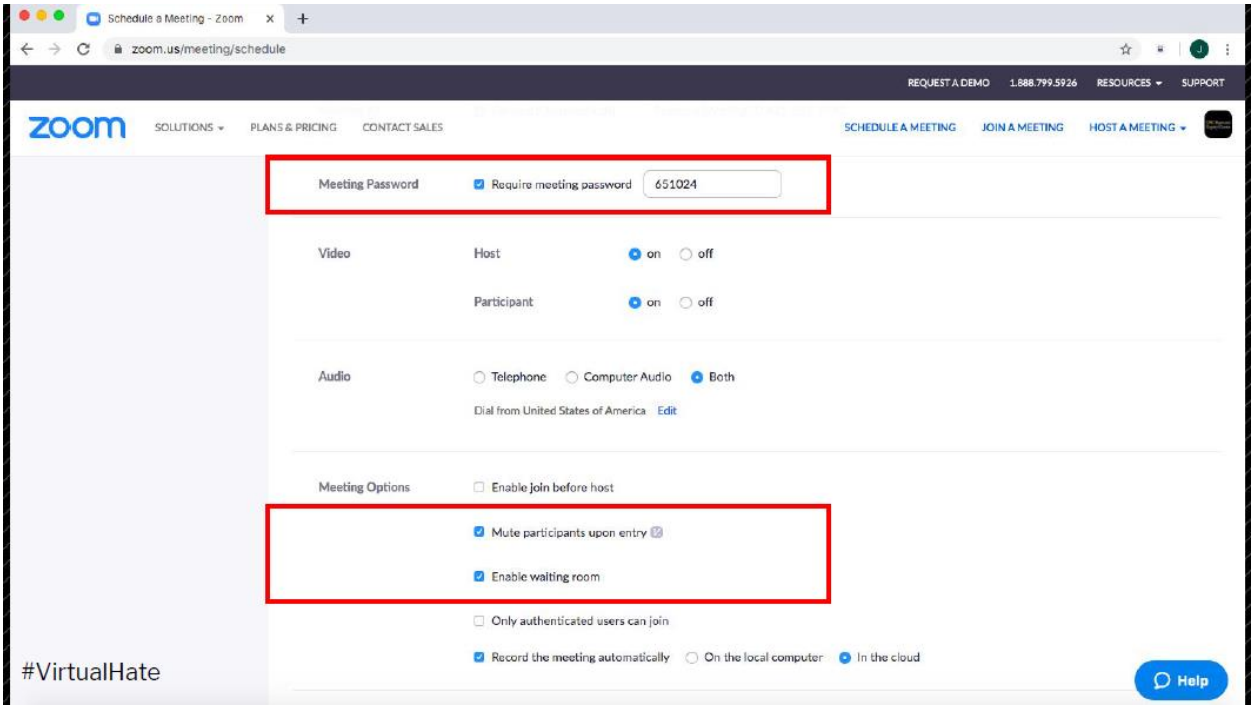
Planning Beforehand

1. Designate someone as a co-host to:
    - Manage the Waiting Room
    - Monitor participant and chat boxes
    - Silence mics if needed
    - Remove ZoomBombers/ZoomTrollers if necessary

2. Let participants know:
    - To arrive 10-15 minutes early for approval to enter
    - Meeting will be locked 5 minutes (or other short time) after the start time
    - If session will be recorded

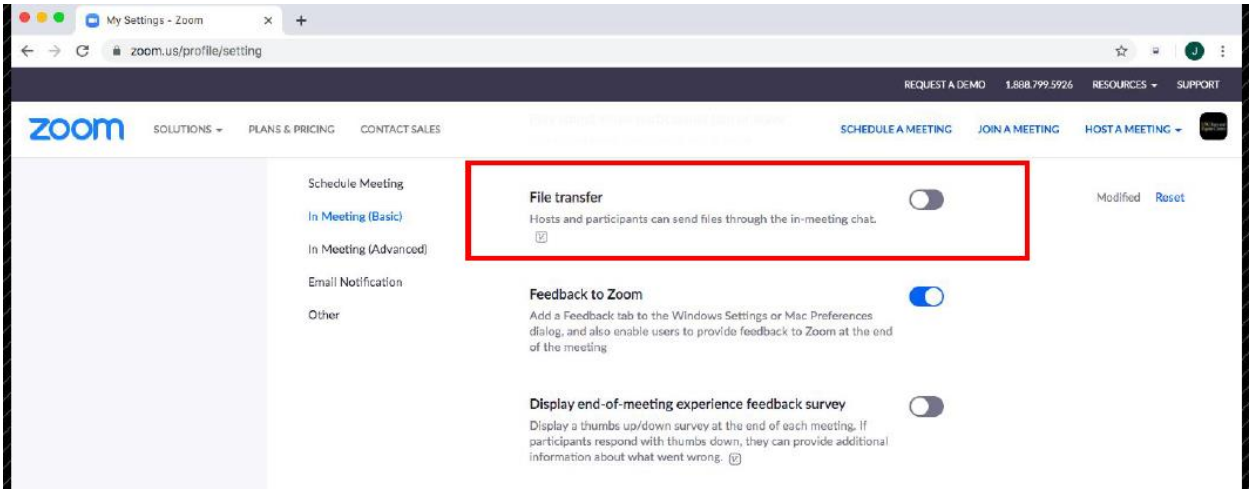
Scheduling

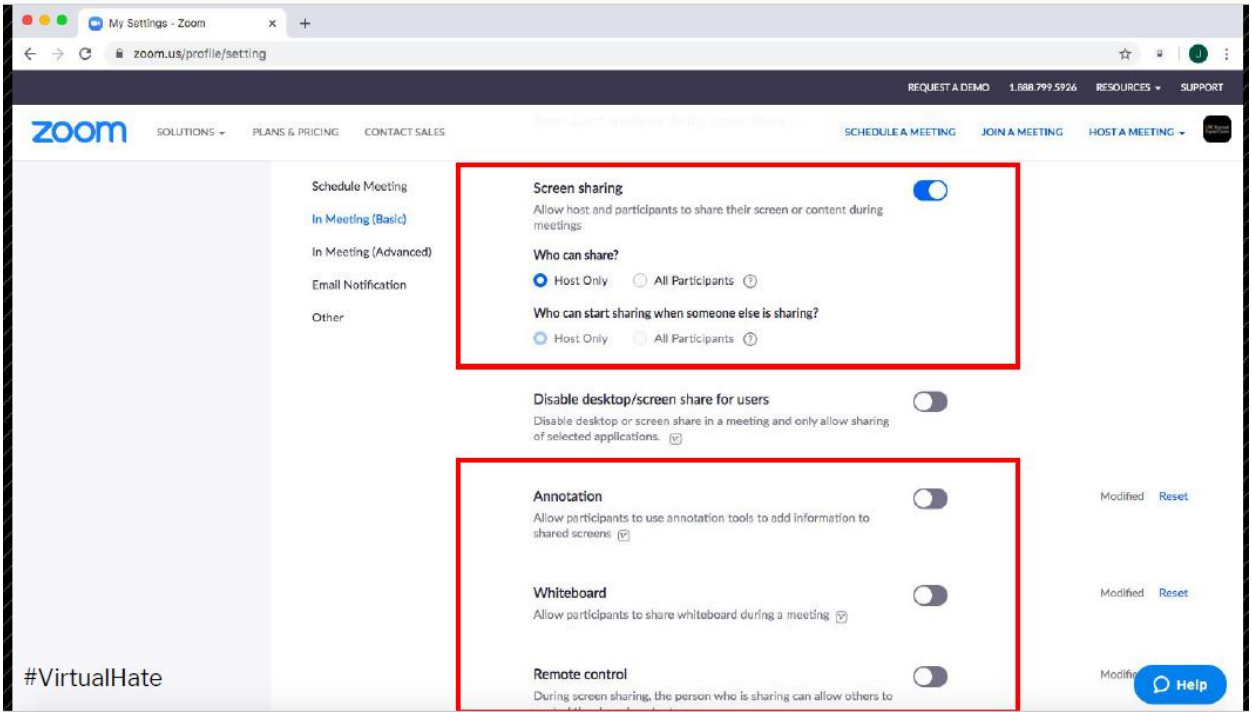
1. When you schedule the meeting…
    - Require a password
    - Mute participants on entry
    - Enable the Waiting Room
    - Do ***not*** share Zoom links publicly (e.g., on Facebook groups, on a website) – share these via email when possible and share the password in a separate email



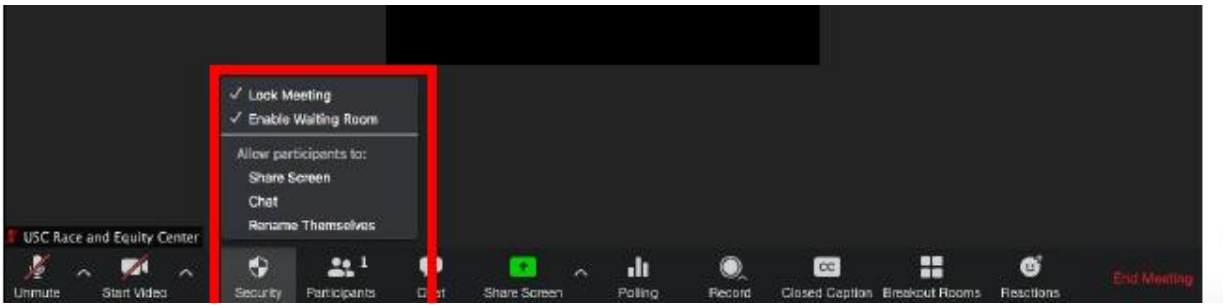
1 Hour Prior

1. Additional Settings
    - Turn off file transfer
    - Screen sharing for host ONLY
    - Turn off annotation, whiteboard, and remote control



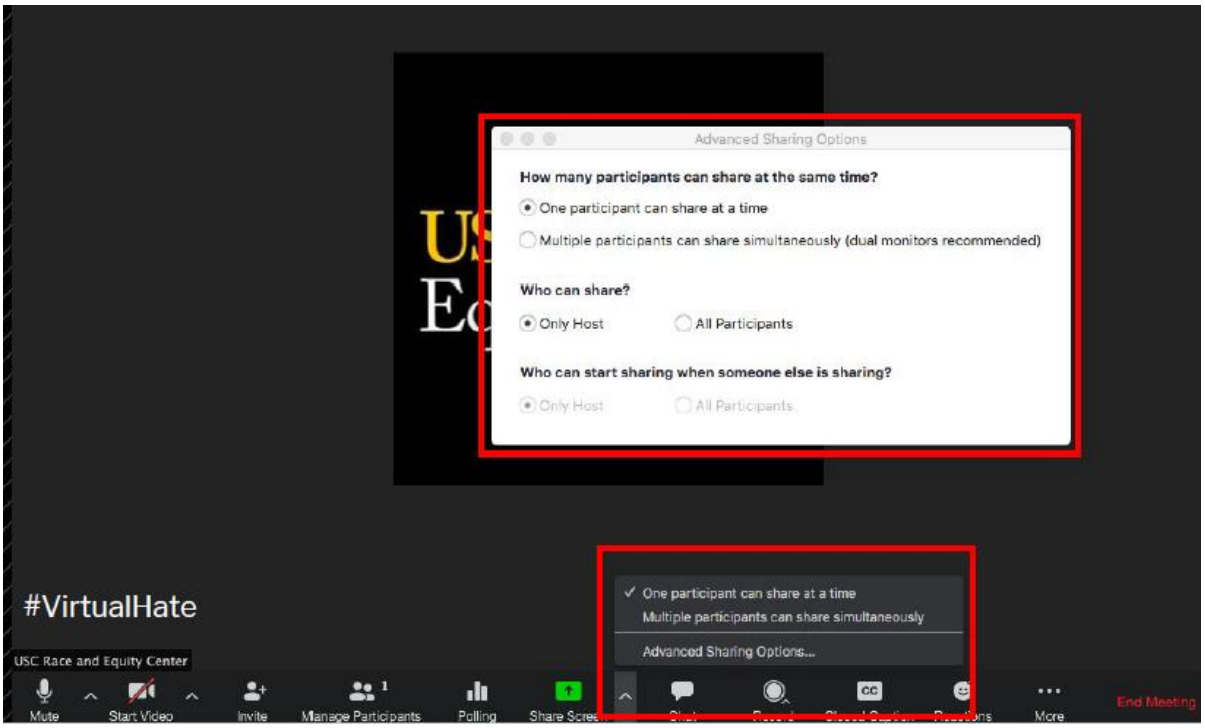


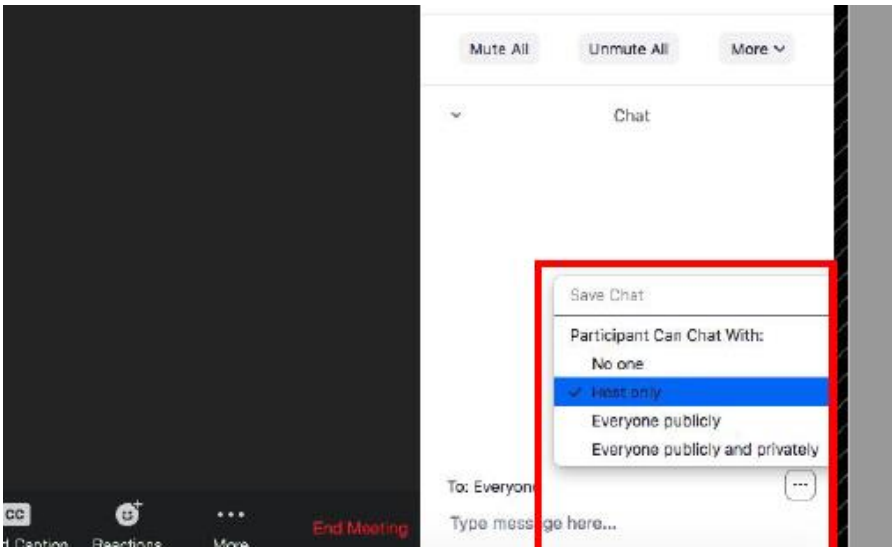
Many of the above options are also available to the host during the meeting through the Security button highlighted in red below

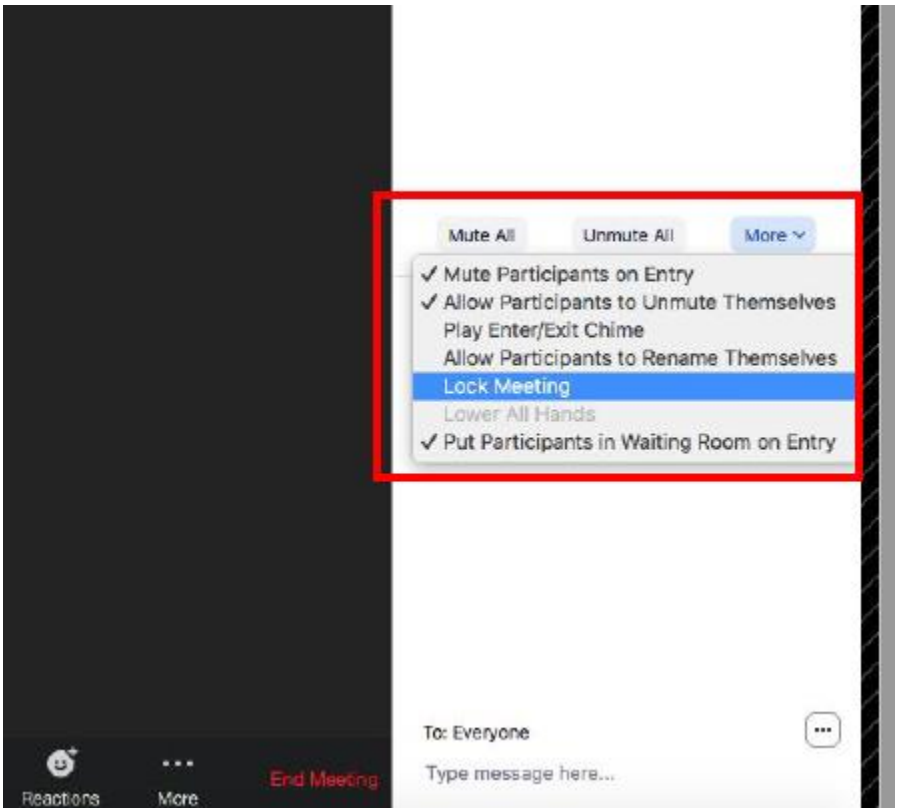


15-20 Minutes Prior

1. Log on early to…
    - Check that Screen Share is set to Only Host
    - Set Chat Box to "Participant can chat with host only"
    - Begin admitting participants from the Waiting Room
    - Lock meeting 5-10 minutes after start time
        - Keep in mind that if someone's internet connection drops, they will not be able to log back in after a meeting is locked, which could create a potential equity issue. Have a protocol available, for example, for participants message the co-host so the room can be momentarily unlocked until they are back in the session. Communicate this protocol with attendees.







We acknowledge that some of these options may not be ideal or desirable in some meetings where cross-group engagement is necessary. For example, limiting the chat box to “Participant can chat with host only” would not be useful in many cases where participants need to message each other or the group during the meeting. Use as many of these options as possible to maximize security, while still allowing for engagement depending on the purpose of the meeting.

Managing in the Moment

PRESENTER	
Stay calm! The impact of Zoombombing/Zoomtrolling on participants is heightened, if the presenter begins to also lose control. Additionally, reactions are being recorded by Zoombombers/Zoomtrollers to share online and to watch later.	Utilize Speaker View to identify the Zoombomber. You can also screengrab without alerting anyone in order to identify the intruders later
Acknowledge what is happening without repeating violent and hateful rhetoric and ask participants to stop their own videos and mute themselves. This can disempower the intruder by not allowing them to see participants' reactions and may also help to identify them if their camera is still on.	Remove the disruptive participants. In speaker view, hover over the person and the three dots on the top right corner allows removal of participant. Or you can hover over their name in the Participant Box.
Check in with participants, minimizing the need to retraumatize each other. Take a couple of collective breaths together to re-center and continue if possible! Perhaps transition with something like, "Let's not give up any more of our time or energy on this right now. I can be available afterwards in case anyone needs space to process what happened. But for now, let's proceed with what was planned."	
Check in with each other and with participants individually (as possible) after the meeting. The impact of these attacks can be long-lasting or triggered later.	

Repairing Harm

Follow Up

1. With Zoom:
    a. Webinar Reporting
    b. Generating Meeting Reports for Registration and Polling
2. Download the chat to address specific comments, to directly name the harm caused to specific communities, without repeating violent and hateful rhetoric (e.g., name "racism" or "anti-Chinese rhetoric" or "homophobia", etc. rather than using the epithets and insults used by the attackers)
3. Acknowledge that what happened was wrong, scary, and unacceptable; connect it to stated/lived community values and broader socio-cultural climate

4. If there are concrete actions that can be taken, take them and then share them with the participants
5. If your Meeting or organization has a bias reporting protocol, report it.

Thinking Through Future Security Needs

These are also some good questions to think through in planning virtual events/meetings.

- Safety team: Ideally focused on security and safety throughout an event/meeting; they should not also be facilitating, moderating, speaking, performing, or presenting.
- What is allowed, expected, and/or tolerated from attendees during the event, and what isn't? This shouldn't be about silencing dissent.
- What are probable threats to the event and the community gathered for it, and how likely is it that those threats will occur?
- How does the community or the organization wish to respond to threats that materialize during the event?

Responses to Q&A during the presentation

I notice that you keep video on for security. Why is that? I thought it might be safer to keep it off so someone couldn't visually share something hateful.

> This recommendation definitely depends on the nature of the meeting. For our purposes, we thought that having participants keep their cameras on provided us with a better sense of accountability rather than having them turned off.

How do you feel about letting phone numbers in, no names?

> While letting phone numbers in with no names feels risky, it can also create an equity issue if this is a program for all students and some students can only dial in by phone. Might be helpful to create a separate protocol for those folks to be able to identify themselves to you directly via email or text.

What if you need to use all of these features for the functioning of your program? We have collaborative learning programs that depend upon allowing participants to be able to participate in these ways.

> Absolutely understandable. Beginning the meeting with all security options in place and then opening it up for set times of interaction might work best. Or, if you are working with a smaller group, consider turning off all security options after everyone has been identified and the meeting has been locked.

What if participants come and do not turn on their cameras? How can I manage that requirement?

> This can change on a case-by-case basis depending on your level of familiarity and comfort with the group.

What happens if Zoombombers take over so completely, you cannot remove them?

> In the case of multiple intruders, it might be possible to announce a 5-minute break to participants and ask them to turn off their cameras and microphones and minimize their Zoom windows while you work to resolve the issue. Beforehand (we know hindsight is always 20/20), try to think about where the line is for you - what would happen that would cause you to terminate the meeting all together? When is there "too much harm" to manage? And be prepared to follow up if you do have to end the meeting.

Other Resources

USC Zoombombing Resources (geared more towards teaching, but still useful)

Zoom's How to Keep Uninvited Guests Our of Your Zoom Event