# Zoom Security and Accessibility

*This document was developed by the ACRL RBMS Diversity Committee in October 2020 and has been adapted with permission for ACRL meetings and forums.*

With the increase in virtual meetings, there are some extra steps you can take to help safeguard your session from Zoombombing. Uninvited guests can potentially "Zoombomb" your room, intimidating participants or causing them to feel unwelcome or uncomfortable, with the insertion of materials that are offensive in nature. There **isn't** a one size fits all solution, but there are some recommended practices and a number of options to consider. Many of these suggestions carry tradeoffs - your participants may not be able to customize their experience in important ways, for instance, so you'll want to assess the risk for your meeting and make decisions accordingly.

## Webinar or Meeting?

If your session requires little interaction between participants, you're probably better off holding a webinar. Webinars are designed for large group meetings with a few speakers. Other attendees are muted by default and cannot unmute themselves, but can be unmuted by the host for comments or questions. Think of webinars like a conference keynote where the presenter speaks for most of the session and attendees line up to be called on for questions. This makes them much easier to secure. If, on the other hand, your session is designed for a small group and is meant to be highly interactive, you might want to schedule it as a meeting. You can find more information on the differences here.

## Requiring Registration

Requiring registration allows participants to register for the session in advance and can be left open during the meeting to allow last minute attendees to join. The one downside of registration is that participants will need to use the desktop or mobile apps as the web interface is not supported. For more information see here.

# Accessibility

Consider the following changes to your meeting settings. You can reach the settings from your web account. In addition to the settings below, we recommend that your event includes captions. We suggest that you have your presenter/s use Google Slides or PowerPoint for Microsoft 365. You will need to open Google Slides in a Google Chrome web browser to have the closed caption feature. However, if presenters choose to use PowerPoint, they'll **need** to have Windows 10. If multiple speakers will be presenting, they'll need to use their computer microphones, (not their headset microphone), so that their voices can be detected as they speak, which is extremely important if there will only be **one** PowerPoint or Google Slides document for all of the speakers.

# Settings

Consider the following changes to your meeting settings. You can reach the settings from your web account.

# Security

- **Enable Waiting Room**. This will allow you to admit each participant individually and filter out users with suspicious or offensive names. People in the waiting room cannot see or interact with each other, so it does not need to be monitored while in this status. If you would like to create a welcoming message for waiting participants click on Customize Waiting Room.

- **Enable Require a passcode when scheduling new meetings.** If this isn't enabled your room is susceptible to Zoombombers targeting URLs at random. The passcode can be embedded in the meeting URL, so it's not necessary for participants to enter it manually.

# Schedule Meeting

- **Disable Participants video.** Participants will still be able to use their camera after they join the room, but it won't be on by default. This gives you more time to react to inappropriate video.

- **Disable Join before host.** You'll want to make sure that you're in the room before anyone can join so that you can monitor for trouble.

- **Enable Mute participants upon entry.** This will prevent participants from immediately flooding the room with inappropriate audio. Participants will need to unmute themselves before speaking.

# In Meeting (Basic)

- **Disable Private chat.** This will prevent participants from harassing other participants in private chat. The host and co-hosts will still be able to chat privately with each other. Use your discretion before you disable this feature.

    - **Disable File transfer.** Highly recommended. If this is enabled, participants can send inappropriate files and display inappropriate gifs in the chat.

- **Enable Co-host**. This will allow you to designate colleagues to help you with hosting abilities, including addressing any disruptive or harmful behavior. You can also make specific colleagues co-hosts when you start your meeting. Simply right click near the person's name, select More and choose the option Make Co-host. There is no limitation on the number of co-hosts you can have in a meeting or webinar.

- If Screen Share is enabled, **select "Host Only" from the Who can Share options. However, if your meeting will have presenters, you'll need to allow participants to share their screen.**

- **Disable desktop/screen share for users.** Screen share permissions can be changed during the meeting if it's necessary for a participant to share their screen.

- **Disable Annotation.** Unfortunately, participants can use this function to leave inappropriate annotations. If this is a necessary tool for your meeting be extra vigilant with it.

- **Disable Whiteboard.** Similar to Annotation, this function has potential for abuse.

- **Disable Remote Control.** Recommended only if you choose to be the only person sharing your screen and do not wish to have another participant in the room the option to request permission to share your screen.

- **Disable Allow removed participants to rejoin.** Highly recommended. Otherwise, Zoombomber can simply rejoin after you remove them.

- **Consider Disable Allow participants to rename themselves.** Participants could name themselves with offensive words. On the other hand, many participants use this feature to change their default name to their preferred name or add their preferred pronouns. This is especially important for transgender people as their organization might use their dead name as their default name. It is probably worth leaving this feature on unless you're holding a very high-risk meeting.

- **Enable Hide participant profile pictures in a meeting.** Zoombombers can set their profile pictures to be offensive or inappropriate images.

## In Meeting (Advanced)

- **Enable Report participants to Zoom.**
- **Disable Far end camera control.**
- **Disable Virtual background.** Zoombombers can set the virtual background to an inappropriate image or video, but participants also frequently use virtual backgrounds in order to not show their surroundings for any number of reasons. **Assess the risks and benefits before making a decision.**
- **Disable Video filters.** While these can be fun, users can also set up inappropriate filters and they aren't necessary.

## Scheduling the Meeting

While scheduling your meeting, consider the following settings.

- Registration: check Required (see above) - Only for larger meetings, not for small business/committee meetings.
- Security: check Passcode and Waiting Room (see above)
- Video: Check Participant off (see above)
- Meeting options
  - Do **NOT** check Enable join before host (see above)
  - Check Mute participants upon entry (see above)

## Promoting Your Meeting

When promoting your event on the open web, do not include the meeting link. Consider requiring registration for the meeting instead, which will disseminate the URL to registered participants. See above for more information.

## Security Tools During the Meeting

See Zoom's website for an overview of the security options available to hosts.

# Tips for Facilitating/Moderating your Meeting

There should be one person dedicated solely to monitoring the event. That person will need to be either the host or a co-host. The monitor can admit people from the waiting room, mute or unmute participants, and if necessary, remove problematic participants.

Make sure to monitor:

- The chat session.
- Participants' video feeds.
- Participant names (if renaming is enabled).

The event should also have a facilitator who explains the guidelines for discussion and ensures all participants are abiding by them.

If you are utilizing breakout rooms, the host will need to stay in the main room in case there are latecomers or somebody's connection is dropped and they have to rejoin. The host will then be able to sort them into a breakout room. Another reason for a host to stay in the main room is in case Zoombombers enter while the rest of the participants are in breakout sessions. For large events with unknown participants each breakout room should also have a facilitator in order to ensure a safe environment.

[**Remember, you are the official gatekeeper of your meeting. This document is meant to serve as an informational tool. Please use your own judgment as to what settings will work best for your meeting. You can make adjustments to your settings, as you deem necessary.]**