How to Secure Meetings in Zoom

Overview

“Zoombombing” is a form of trolling that disrupts online meetings and classes with disturbing language or images through screen sharing. As reports of Zoombombing rise, UB is taking proactive measures to ensure our meetings, classes, and community are protected.

We highly encourage our community to do everything possible to secure their meetings, participants, and data, and recommend the following methods of securing your Zoom meetings. See our Quick Start Guide: Securing Meetings in Zoom for more information.

How You Can Secure Your Meetings

Meeting Settings:

- Restrict your meetings to **Only Authenticated users can join**. When scheduling a new meeting in the web browser, you have the ability to choose to restrict users not logged in through the UB domain to join a meeting or restrict users not authenticated to Zoom.
- Enable **Require a password when scheduling new meetings or webinars** through the **Meeting** tab of your Settings. Participants will then be required to enter a password to join the meeting. See Meeting and Webinar Passwords for more information.
- Send participants to the **Waiting Room**. (Meetings only) Only the host can allow participants in the **Waiting Room** into the live meeting. See Waiting Room for more information.
- Disable **Join before hosts** to ensure participants are not able to join the meeting before the host arrives. See Scheduling meetings for more information.
- Disable **In Meeting Chat** through your **Profile** settings. Here you can toggle off allowing participants to chat. This is also where you can prevent users from saving chat. See Disabling In-Meeting Chat for more information.

- Ensure only hosts can share their screen through Settings by un-checking **Participants** under **Who can Share?** See Managing participants in a meeting for more information. This is on by default.
- Disable **File Transfer** in **Settings**, which will ensure participants are not allowed to share files in the in-meeting chat during the meeting. See In-Meeting File Transfer for more information.
- Stop a participants video stream to ensure participants are not on video through **Manage Participants**. See Managing participants in a meeting for more information.
- Click to **Mask phone numbers in the participant list** through the **Telephone** tab in Settings. This masks all telephone numbers called into the meeting.

Settings when scheduling your meeting or webinar:

- **Mute** all participants that are already in the meeting and new participants joining the meeting through Manage Participants. You will be asked to confirm if you'd like to allow participants to unmute themselves. You can choose to uncheck this option. See Mute All And Unmute All for more information.
- **Lock your meeting** allows hosts to lock the meeting right at the start (or when enough attendees have joined). At the point a meeting is locked, no other participants are able to join the meeting. See Can I Restrict My Meeting Capacity for more information.
- Put participants **On Hold** through Manage Participants while in a meeting. When a user is put on hold, they will be taken out of the meeting until the host clicks to take the user off hold. See Attendee On Hold for more information.
- **Disable private chat** through Manage Participants. This prohibits participants from private chatting with other participants. See In-Meeting Chat for more information.

Other suggestions for ensuring a secure meeting:

- Do not publish URL in public communication channels
- Remind participants to not share meeting details

See Host and Co-Host Controls in a Meeting for more information on meeting controls.