HOW TO SECURE MEETINGS IN ZOOM

QuickStart Guide

1. HOST: Use your ".edu" email address, no personal email addresses.
2. HOST: Set a meeting password.
    a. Zoom states that passwords and waiting rooms are turned ON by default as of 5 April.
    b. To avoid defaults, cancel the existing invite off of our calendars and create a new invite - just to be sure.
3. HOST: Prevent Zoombombing: If you schedule a meeting from the web interface, you won't see the option to disable screen sharing. Instead:
    a. Click on "Settings" in the left-hand menu
    b. Scroll down to "Screen sharing" and under "Who can share?" click "Host Only"
    c. Click on "Save"
    d. Once you save your settings, future meetings that you start will have sharing disabled by default.
4. HOST: Changing settings after the meeting has started:
    a. Once your Zoom meeting is running, click the caret to the right of the green "Share Screen" button in the center of the bottom row of icons.
    b. Click "Advanced Sharing Options..."
    c. A dialog box will pop up allowing you to switch screen sharing availability from all participants to the host only.
5. ALL: Do not share a link to a teleconference or classroom on an unrestricted publicly available social media post. Provide the link directly to specific people.
6. ALL: Use only the updated version of remote access/meeting applications.

Meeting Settings

"Zoombombing" is a form of trolling that disrupts online meetings and classes with disturbing language or images through screen sharing. Visit Zoom for comprehensive instructions.

- https://blog.zoom.us/wordpress/2020/03/20/keep-uninvited-guests-out-of-your-zoom-event/
- Zoombombing
    - Best Practices for Securing Your Virtual Classroom, Zoom Blog. March 27, 2020
    - 'Zoombies' Take Over Online Classrooms, Inside Higher Ed. April 3, 2020
    - Zoombombing: What it is and how you can prevent it in Zoom video chat, Cnet. April 3, 2020
- The most important thing you can do to secure your meetings restrict to **Only Authenticated users can join**.

- Enable **Require a password when scheduling new course/meeting** 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.
- 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.
- Ensure only hosts can share their screen through Settings by un-checking **Participants** under **Who can Share?**
- Disable **File Transfer** in **Settings**, which will ensure participants are not allowed to share files in the in-meeting chat during the meeting.
- Stop a participant's 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.

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

Recent Update

New Version 4.6.20033.0407 is available. Release Notes: Changes to existing features are:

- Remove meeting ID from the title bar.
- Move invite button to Participants panel.
- Add Security button in the host's meeting toolbar