Recommendations for Zoom Security Settings

Public Meetings

The nature of public meetings is to be inclusive and allow members of the community to join and participate in the meeting. *Please note, any meeting links that are publicized on web pages will be accessible to any individual who browses to that website.* The use of a password on such a publicized meeting will not keep out unwanted participants.

Special note: If you are hosting large public meetings it is recommended you use 'Zoom Webinar' to host that meeting; this allows for greater control and features of your meeting. You may request a webinar account by going to the webinar request form.

All Meetings

The following features will help assist you in securing your larger meetings, such as seminars, with your regular Zoom account.

- Under Settings, select "View More Settings" – This will take you to the website where you can set the following default settings prior to creating your meeting:
    - Enable **Waiting Room Feature** - This feature requires you to actively monitor those in the waiting room and let them in. Waiting Rooms can be customized. For large gatherings it's recommended to have multiple administrators monitoring the waiting room other than the primary presenter. This can be done by enabling "Co-Host"
    - Disable **Join before Host** - do not let participants join the meeting before the host of the meeting actually arrives.
    - Disable **Use Personal Meeting IDs** - these IDs will persist between your meetings and can be potentially used to access meetings in the future.
    - Enable **Mute participants upon entry** - if at any time during your meeting participants are being disruptive, select the "Participants -> Mute All" button to silence the disturbance
    - Disable **Public chat**, if there is to be no feedback or chatting needed within a meeting – this is another method used to cause disruption in meetings
    - Disable **Sound notification when someone enters** - can be distracting when hosting large meetings
    - Disable **Allow file transfer** – unless there is a specific need
    - Enable **Feedback to Zoom** – This allows users to give feedback on the meeting experience
    - Enable **Co-Host** – For larger meetings where assistance is needed to manage participants
    - Enable **Screen sharing** and set to **Host Only** - it's highly recommended to disallow All Participants the ability to share within a public meeting
    - Enable **Disable desktop/screen share for users** – this prevents users from sharing their desktop
    - Disable **Annotation**, if this is not a feature that is needed for your meeting (this is a common method used to disrupt meetings)
    - Disable **Whiteboards**, if this is not a feature that is needed for your meeting
    - Disable **Remote Control**, if this is not a feature that is needed for your meeting
    - Enable **Nonverbal feedback -** This allows participants to interact without disrupting the meeting flow
    - Enable **Meeting reactions** – This allows participants to interact without disrupting the meeting flow
    - Disable **Allow removed participants to rejoin** – This prevents any users removed from a meeting to rejoin
    - Disable **Allow participants to rename themselves** - To prevent offensive names from being displayed
    - Enable **Report participants to Zoom -** This setting will be enabled under the Security feature of a meeting and allow you to submit disruptive behavior to Zoom directly
    - Disable **Far end camera control** - this will prevent users from controlling the hosts camera
    - Enable **Identify guest participants in the meeting/webinar** - this allows for users not part of UChicago or UChicago Medicine to be identified as a guest within the meeting, which could be important for identifying disruptive behavior

    - Disable **Allow live streaming meetings** - in order to ensure meetings are not subsequently streamed through other channels, such as Facebook.
- Under **Recording:**
    - Disable **Local recording** – unless a requirement for the meeting. If allowed decide if permission is required.

While in a meeting the follow settings can be used:

- Under Security:
    - **Lock Room** – this keeps any new participants from joining
    - **Enable Waiting Room**
    - Disable **Allow participants to:**
        - **Rename Themselves**
        - **Share Screen**
        - **Chat**
- Under **Share Screen** -> **Advanced Sharing Options:**
    - **Only Host**
- Under **Participants** click on the ellipsis (…)
    - Disable **Allow Participants to Unmute Themselves** – this allows Host only to allow participants to speak.
    - Other options allow to change some of the previous settings on the fly.
    - **If a participant becomes disruptive** click on the ellipsis (…) next to their name and select **Remove**
- Disable “Join different meetings simultaneously on desktop”; this will limit users who are attempting to disrupt multiple meetings at the same time