Instructor Guide: Preventing Zoom Disruption

To make meetings as secure as possible, there are best practices and optional settings the host can pre-select on their Zoom profile page for additional security and control.

Best Practices for Secure Zoom Meetings:

1. Ensure the meeting link is not posted publicly (outside of Canvas or any legitimate class communication).
2. Ensure either a passcode and/or waiting room is set for the Zoom meeting. Passcodes are automatically enabled for all UBC Zoom links.
3. Review How to Defuse Zoom-bombs. Please note this article mentions the security icon; that has now changed in Zoom to the "Host Tools" icon. If possible, consider having someone assist you in moderating the session – especially for large class sizes.

Recommended Zoom Profile Settings

Click on **settings** on the left-hand side when you log in to the UBC Zoom site. These must be set before meetings are created; they will not affect meetings that have been created prior to the changes. Note this may restrict creative expression for participants.

- Under "In Meeting (Basic)" settings:
    - **Remote control** – turn off (de-select) the **'Allow "auto accept all requests"** option so that guests cannot take over the screen sharing content without permission.
    - **Allow users to change their name *when joining* a meeting** – de-select this to ensure users are joining under their real name. Note: the student's Zoom profile information is shown – including name & pronouns.
    - **Allow users to rename themselves** – de-select this to disallow students changing their name *after they have joined*. It will show what information is in the student's Zoom profile, including name and pronouns. This can also be changed during a meeting using host tools but its better if done before.
    - **Hide participant profile pictures in a meeting** – turn this on to guard against profile pictures being used to disrupt the Zoom meeting.
- Under "In Meeting (Advanced)" settings:
    - Turn off **Allow anonymous questions** to enhance accountability.

If you do experience a situation where a disruptor gains access to your Zoom session, please contact the UBCO Centre for Teaching and Learning so we can guide you to the best next steps.