Zoom – Best Practices (from UBC IT)

As many of us are using Zoom to continue our operational work, it is important to keep a few best practices in mind to prevent unwanted activity from interrupting classes and meetings. Increasingly prevalent is Zoom bombing, where during a class or meeting, intruders hijack the session by saying or showing inappropriate content. Zoom bombers who are successful in disrupting sessions can also post video footage of the incidents to video sharing platforms. To help prevent this, use Zoom meeting best practices:

- **Avoid sharing meeting links on social media or anywhere public.** When you, or other invitees, share your meeting link on social media or other public forums, that makes your event open to anyone in the world with the meeting link and details
- **Manage screen sharing.** To prevent people from sharing unwanted images, restrict sharing to the host.
- **Introduce a waiting room.** One of the best ways to use Zoom for public events is to enable the waiting room and only admit those who you know and are expecting
- **Lock the meeting.** Once all participants have arrived, lock the meeting to prevent uninvited guests.
- **Manage participants.** Be familiar with how to mute or remove participants and disable video.

If you experience Zoom bombing, report the incident to the Cybersecurity team at security@ubc.ca and to Zoom.

For more information and full details on how to use the features listed above, visit https://it.ubc.ca/services/teaching-learning-tools/zoom-video-conferencing/zoom-privacy-and-security-settings#zoombomb