Notice about Data Mining

Zoom has the standard practice of data-mining. Zoom data mines all information provided on their service, so sensitive and/or confidential information should not be shared on Zoom.

There are also reports that Zoom is capturing the 'tabs' that are open on the browser that you are using Zoom on. Use a private/incognito browser for Zoom and refrain from opening any additional tabs within that private/incognito browser.

Mitigating the risk of 'Zoom Bombing'

What is 'Zoom Bombing'?

Zoom Bombing is when an unwelcome stranger enters into your Zoom meeting as a participant disrupts the meeting in a number of ways:

- Being disruptive on the mic
- Presenting unwelcome cam video
- Presenting and/or sharing unwelcome materials (images, movies, slides, etc.)
- Annotating over top of your presentation

What can I do to mitigate the risk of 'Zoom Bombing'?

When setting up your meetings consider using the following:

- Ensure **"Join Before Host" is <u>disabled</u>** - No one can join the session before the host is there.
- Ensure **"File Transfer" is disabled** - Malicious files cannot be distributed (we recommend using file shares / cuLearn / Microsoft Teams / OneDrive).
- Consider allowing aother to help moderate Zoom sessions. To do so, ensure **"Co-Host" is enabled**.
- **Ensure "Allow Removed Participants to Re-join" is disabled** - Individuals who have been kicked out of the session cannot slip back in.

To further protect Zoom sessions, instructors and other session hosts can disable screen sharing for attendees. Screen sharing is allowed by default to improve the ease of use for remote work and learning, but **we highly recommend you turn screen sharing off if it will not be necessary**.

Disable screen sharing for your meeting attendees

1. **Sign In** to configure your account.
2. On the left side of the page, click **Settings**.
3. Under *Screen Sharing* select **Host Only**.

Other considerations:

- Avoid using your Personal Meeting ID (PMI) to host public events. Your PMI is essentially one continuous meeting and people can pop in and out all the time
- Familiarize yourself with Zoom's settings and features. Understand how to protect your virtual space. e.g., **use a Waiting Room**. The waiting room is a helpful feature for controlling attendees.
- This is useful if you want to control your guest list by invite only. For example:
  - **Lock the meeting**: When you lock a Zoom Meeting after it has started, no new participants can join, even if they have the meeting ID and password (if you have required one). In the meeting, click Participants at the bottom of your Zoom window. In the Participants pop-up, click the button that says Lock Meeting.
  - **Set up your own two-factor authentication**: You don't have to share the actual meeting link. Generate a random Meeting ID when scheduling your event and require a password to join. Then you can share that Meeting ID through a public setting/social media and only send the password to join by email or direct message.
  - **Remove unwanted or disruptive participants**: From that Participants menu, you can hover over a participant's name, and several options will appear, including Remove.
  - **Allow removed participants to rejoin**: When you do remove someone, they can't rejoin the meeting. But you can toggle your settings to allow removed participants to rejoin, in case you remove the wrong person.
  - **Put them on hold**: You can put each participant on a temporary hold, including the attendees' video and audio connections. Click on someone's video thumbnail and select Start Attendee On Hold to activate this feature. Click Take Off Hold in the Participants list if/when you're ready to have them back.
  - **Disable video**: Hosts can turn someone's video off. This will allow hosts to block unwanted, distracting, or inappropriate gestures on video.
  - **Mute participants**: Hosts can mute/unmute individual participants or all of them at once. Hosts can block unwanted, distracting, or inappropriate noise from other participants. You can also enable Mute Upon Entry in your settings to keep the noise down in large meetings.
  - **Turn off file transfer**: In-meeting file transfer allows people to share files through the in-meeting chat. Turn this off to keep the chat from getting unwanted content.
  - **Turn off annotation**: You and your attendees can doodle and mark up content together using annotations during screen share. You can disable the annotation feature in your Zoom settings to prevent people from using it.
  - **Disable private chat**: Zoom has in-meeting chat for everyone or participants can message each other privately. Restrict participants' ability to chat with each another during your meeting. This prevents anyone from getting messages during the meeting.
- **Use a Waiting Room**
  - One of the best ways to use Zoom for public events is to enable the Waiting Room feature. The Waiting Room is a virtual staging area that stops your guests from joining until you're ready for them, like a bouncer carefully monitoring who gets let in.
  - Meeting hosts can customize Waiting Room settings for additional control, and you can even personalize the message people see when they hit the Waiting Room so they know they're in the right spot.
  - The Waiting Room is really a great way to screen who's trying to enter your event and keep unwanted guests out.