Securing Zoom Meetings

Zoombombing is when an uninvited guest joins a meeting or class on the popular web-conferencing platform Zoom and uses its screen-sharing feature to bombard attendees with inappropriate material. It is completely counter to the University of Iowa's core values, which include diversity and respect. The UI Office of Teaching, Learning, and Technology recommends taking these steps to secure your Zoom session and help prevent unwanted guests from disrupting your online event.

Update Zoom

It's important that you're running the most recent version of Zoom. This ensures that you have the most updated controls when hosting or joining a meeting.

Share link privately

Privately sharing the meeting link to your participants (via email, ICON, etc.) is a good way to ensure the link isn't publicly available. Avoid sharing the link on social media.

Set a meeting password

Requiring a password is a straightforward way to increase the security of your meeting. Send the password to your attendees, but be sure to remind them not to share it.

Remove guests from room

If you find an unwanted attendee has joined your session, you can mute them and remove them from the meeting.

Lock a room

Using Zoom Host Controls, you can lock a meeting once all attendees have joined. When a meeting is locked, no one can join, and the host will not be alerted if anyone tries to join.

Control screen sharing

By default, only the host of a meeting can share content. To allow participants to share content, you will need to enable that in your user settings.

More information is available here: **teach.uiowa.edu/zoom-security**.

If you have questions, please contact the ITS Help Desk. ☎ 319-384-4357 ✉ its-helpdesk@uiowa.edu 💬 helpdesk.its.uiowa.edu/connect