

Zoombombing Prevention Cheat Sheet for Faculty

Summary of Touro Zoom Security Advisory Announcements (April 7, 2020)

- Do not make meetings or classrooms public.
- Do not share a link to a teleconference or classroom on an unrestricted publicly available social media post. Provide the link directly to specific people.
- Don't use the same meeting ID between Administrative or Confidential meetings and Classroom meetings.
- Avoid starting public events using your Personal Meeting ID (PMI) because your PMI is basically one continuous meeting and you don't want others crashing your personal virtual space after the your meeting is over.
- Generate random meeting IDs.
- Require a meeting password.
- Use the waiting room feature and control the admittance of guests.
- Zoom's 'Share Screen' function is being restricted to meeting hosts and co-hosts only. This means that only the meeting host and designated co-hosts are able to share their screen with participants. If you are hosting a Zoom meeting in which certain participants are required to share their screen, please follow these steps to temporarily grant them access to share:
 1. Go to the Participants list
 2. Click the 'More' button next to the participant's name
 3. Select 'Make Co-Host'
 4. Inform the participant they are now able to share their screen

To revoke the access to share:

1. Go to the Participants list
2. Click 'More' button next to the participant's name who is a co-host
3. Select 'Withdraw Co-Host Permission'

As the Zoom meeting host, you may assign, revoke, and re-assign the role of meeting co-host as necessary during your meeting.

- Disable private chat.
- Turn off file transfer.
- Turn off annotation.
- Allow only signed-in users to join.
- Lock the meeting after all participants have logged on.
- Other suggestions:
 - Remove unwanted or disruptive participants.
 - Prevent removed participants from rejoining.
 - Put participants on hold.
 - Disable video.
 - Mute participants.
 - Be sure you are using the latest version of Zoom. Zoom automatically updates their software.
 - Be sure that these updates are happening on your computer or phone. You can see the version of your software in your Zoom settings. Check for the latest version available on the zoom.us website.