Recent incidents of unauthorized access to open online synchronous classes have caused significant distress for instructors and students. These so-called "Zoombombers" are using publicly available web meeting links to infiltrate online classes and share offensive, obscene, violent and racist content and imagery. While the reported incidents have specifically involved Zoom, other platforms that support public meeting links such as WebEx could also be susceptible.

Prevention

- **Recommended:** Use Microsoft Teams to schedule synchronous web meetings for office hours or other needs. Create a link to the meeting on Canvas. Recurring meetings use the same link for every occurrence. Participants will need to authenticate with their *eID*@colostate.edu login to participate.
- Use Canvas Conferences for office hours. However, understand that our license for Canvas Conferences is limited and depending on usage, may not be available.
- Change web meeting settings to control access and sharing. Consult vendor's support resources for information about these settings.
    - Don't allow participants to screen share without permission.
    - Generate a meeting ID and post only in Canvas or in email directly to students
    - Remove anonymity. Require authentication or providing a verifiable email address.
    - Turn off participant video, file transfer, private chat, and other ancillary features if not needed.
    - Use a "waiting room" to control participant access.
- Create norms for participating in web conferences. Similar to creating an ideal classroom climate for learning, set expectations and operating norms to facilitate a positive learning experience.

Resources

Zoom: https://blog.zoom.us/wordpress/2020/03/20/keep-the-party-crashers-from-crashing-your-zoom-event/

WebEx: https://help.webex.com/en-us/8zi8tq/Cisco-Webex-Best-Practices-for-Secure-Meetings-Hosts

https://www.internet2.edu/news/detail/17600/

https://www.pcmag.com/news/fbi-watch-out-for-zoom-bombings-on-online-video-meeting-apps