UHM College of Education

Zoom Security Strategies For Student-Led Presentations

In order to discourage Zoombombing and phishing attacks, you can use any or all of the following strategies.

**Before Presentation**

- When scheduling in Zoom enable the following settings:
  - Enable Password - See [Scheduling meetings](#) for more information. You can copy a special link with the password embedded in the link (see screenshot).
    
    ![Meeting Password](https://example.com)
    
    - Set Meeting ID to Generate Automatically - See [Scheduling meetings](#) for more information.
    
    ![Set Meeting ID](https://example.com)
    
    - Set Video off for both host and participants
    
    ![Video Settings](https://example.com)
    
    - Set Meeting Options to Mute participants upon entry and Enable waiting room
    
    ![Meeting Options](https://example.com)
- Send the announcement to the appropriate listserv using the Gmail confidential mode - See [Send & open confidential emails](#).

- Avoid advertising the Zoom link publicly. This includes social media platforms such as Facebook and Twitter.
- You can also require registration. See [Register for Meetings](#).

### During Presentation

- Designate a co-host to minimize disruptions during the Zoom session. Their duties will include:
  - If the waiting room is activated, screen for potential disruptors (fishy or inappropriate names) and admitting all the other participants.
  - Mute participants’ mics or video if necessary
  - Remove participants if they are disruptive.
- Disable participant sharing and elevate your student to co-host
- Disable chat during the presentation then enable during the Q&A session
- Remind participants to avoid visiting any web links posted in chat (this could be possible phishing).
- If your student needs to share links with participants, encourage them to use [bit.ly](https://bit.ly) or [go.hawaii.edu](https://go.hawaii.edu) to shorten their links and put them on a presentation slide.
- At the beginning of the session, share with participants that for security reasons:
  - Chat will be disabled during the presentation and it will be enabled during Q&A
  - Participants should avoid posting web links in the chat or going to links in the chat during Q&A.
- These options can be found in the Zoom Security Menu:

  ![Zoom Security Menu](#)

  For more info, see [In-meeting security options](#)

These resources are provided by Zoom and COE Technology and Distance Programs