Security of ZOOM Meetings for Invigilated Online Examinations

Apr 29, 2020

Background

In the document "Recent alerts on ZOOM and suggested actions (last updated on Apr 27)", we have provided updates on ZOOM security alerts and suggested actions for CUHK ZOOM users including best practices for online classes and open events involving the general public. This document sets out details of technical measures to prevent disturbance during online examinations caused by unauthorized access and address concerns about privacy. All teachers are strongly advised to adopt these measures in setting up their online examinations, and the "waiting room" function will be set as a default for all Zoom meetings with effect from 4 May 2020, which will apply to invigilated online examinations. Teachers who have very special reasons can choose to opt-out from this default setting.

Technical measures to prevent meeting disturbance caused by unauthorized access and address concerns about privacy

1) Do not share the meeting link on social media or publicly (e.g. on websites).

2) Update ZOOM clients/app to the latest version.
   - On Apr 27, 2020, ZOOM released ZOOM 5.0.
   - After May 30, 2020, all ZOOM clients on older versions will be required to upgrade before joining meetings.

3) Enable the Waiting Room and use **Remove Participant…** if needed
   - When enabled, all participants will be sent to the waiting room, where you can admit them individually or all at once.
   - *Important: Starting May 4, 2020, the Waiting Room feature will be automatically turned on by default. If you have created your meetings before May 4, please review and enable this option for the protection.*

4) Inform students that you will only admit them if they use their official name (as in CUSIS) to join the meeting.
   - If needed, consider asking students to add no more than the last 3 digits of their student id number after their name for additional checking.

5) If needed, remove participants who have caused meeting disturbance.
   - Even if a particular participant tries to re-enter, the participant can only wait in the waiting room.

6) Use breakout room(s) for private exchanges with students
   - Select to assign participants into the breakout room(s) manually
   - Configure "chat to host only" and ask students to use "raise hand" or "chat" to get your attention so that you can manually assign them to a breakout room for private exchange.

7) Review and adopt additional best practices suggested by ZOOM for securing virtual classroom (if they are applicable to the invigilation arrangement).
   a) Lock your virtual classroom
   b) Control screen sharing
   c) Lock down the chat
   d) Adopt security options when scheduling a class
      i. Require registration
      ii. Use a random meeting ID
      iii. Password-protect the classroom
      iv. Allow only authenticated users to join (domain: *.cuhk.edu.hk)
      **Some users in ML China reported difficulties with the login steps in April 2020*
      v. Disable join before host
      vi. Manage annotation
      vii. Attendee on-hold

8) Review and adopt additional Information Security Best Practices published by ITSC regularly.

9) Please contact elearning@cuhk.edu.hk if more information is needed.