QUICK GUIDE FOR ZOOM SECURITY

Health System Sustainability
NHMRC Partnership Centre

Zoom video meetings are encrypted, and this protects their contents from being intercepted by third-parties. While Zoom do hold the decryption keys and can theoretically decrypt meetings, this should only occur when cloud recording of video meeting is enabled, or a telephone or SIP/H.323 room system joins the meeting.

Zoom video meetings are vulnerable to unwanted intrusion if some practices are not followed. The following safeguards are easy, yet effective, ways to reduce intrusion of your Zoom video conference. Access to these security settings will depend on your Zoom interface and operating system.

Follow these tips to increase Zoom security

Use the waiting room

The waiting room feature prevents participants from joining a meeting until they have been granted permission by the meeting host. Participants in the waiting room will not be able to interact with each other, or with the meeting. The waiting room option can be enabled when the meeting is scheduled, or by editing an existing meeting.

Lock the meeting

Once the meeting has started and all participants are present, the meeting host can lock the meeting to prevent anyone else from joining.

✱✱✱✱ Use a meeting password

By default, only the meeting ID is required to join a Zoom meeting. Meeting IDs are 10 or 11-digits and while the chance of someone guessing your meeting ID is extremely low, there are attackers that actively search the internet for publicly advertised meetings, with the intention of causing disruption.
Passwords add a second layer of security to meetings. When a password is being used, do not advertise it alongside the meeting ID. Instead, communicate it to meeting participants in-person or in a separate email. While password-protecting a meeting is not always practical, it should be done whenever possible. The meeting password can be set when the meeting is being created.

Only advertise meetings where necessary

Never share private meeting details over public social media. Examples of this could include posting a meeting invitation on a friends' Facebook page, or replying to a colleague's Twitter post with a link to a private Zoom meeting. Only the intended meeting participants should have access to the meeting details, and invitees should be reminded to not share these details with anyone else.

Mute or remove disruptive participants

The meeting host can mute the video and/or audio of participants, or remove them from the meeting via the participants panel within the Zoom interface. The meeting host should ensure that they are logged-in to Zoom when joining the meeting, and/or have granted co-host privileges to another meeting participant, so that these options are available.

Avoid re-using meeting IDs

Generating a new meeting ID for each meeting will prevent attackers from joining and interrupting meetings using old meeting details. This functionality can be enabled when the meeting is being scheduled.

CONTACT US: coh.centre.uq.edu.au enquiries@coh.uq.edu.au @UQ_COH

Version: April 2020