

Protect your Zoom meeting from 'zoombombing'

Slides available at <http://tiny.cc/ypklnz>

Most of these security features are already enabled when you create a zoom meeting. These notes will help you understand what is controlled and how

Schedule your meeting - send your participants their invitation by email

Use the Zoom process for scheduling, making sure that you 'generate automatically' both a meeting ID and a password

Email the meeting ID and password to your participants

This is a one-off code each time

If you are cut off mid-meeting after 30-40 minutes free time repeat the process of generating an automatic ID and password. The one you just used will not work.

'Enable waiting room' under advanced options

'Enable waiting room' is checked by default, meaning your meeting is automatically secure. This means the meeting host has to 'admit' attendees as they sign in. Depending on your meeting size you can admit one at a time or admit all.

The host will see a pop-up notice every time someone wants to come in. You can check who the person is and refuse to admit them if they are unknown.

Lock your meeting when everyone has arrived

As host, you will see a shield icon in your tray of tools.

When your guests have all arrived, click on the shield and choose 'lock meeting'

Nobody else can apply for admission after you do this

If an incident occurs - worst case scenario

We stress that the security measures above will keep you safe. If your meeting is attacked in any way, the host should immediately end the meeting.

Click on the words 'end meeting' at bottom right, and '**end meeting for all**'

Make a note of the time and date of the incident

Forward a quick summary including time and date of incident to Zoom and to your U3A chair