Being Secure: ZOOM Best Practices at Western Sydney University

Your choice of settings when scheduling and hosting Zoom will give you a well-controlled environment right from the start, helping to ensure your security. As the host of a meeting, it is important that you check your ‘meeting settings’ before you start.

1

Be a Good Host: Take Control with your Settings

- Adjust your Default Zoom meetings (login at https://uws.zoom.us)
- Set Screen Sharing in your Zoom ‘Settings’ to ‘Host Only’. You can enable participant screen sharing once in the meeting if and when you need it.
- Turn Enable Join Before Host to OFF
- Mute Participants on Entry to ON
- See Zoom's Managing participants in a meeting guide
- For more advanced security where you can limit and monitor attendance by using WSU Sign In, please contact the IT Service Desk for more information about this feature.

2

Always make sure your Software is Up-to-Date

- Make sure you’re using up to date software https://uws.zoom.us/download - it’s both more secure and enables extra features.

3

Use a Different Meeting ID

- Do not use one Meeting ID for everything. Schedule a different, but recurrent Meeting ID meeting for each timetabled session. Delete these after the end of semester and create new ones for the following semester.

4

Require a meeting Password

- This will help to prevent Zoombombing and other interruptions from non-invitees: https://zoom.us/security

WESTERN SYDNEY
UNIVERSITY