AVOID ZOOMBOMBING

ZoomBombing as reported on threatpost refers to interruption of zoom video-conference meetings by uninvited unscrupulous and malicious people. Such malicious people get access to such meetings through publicly shared meeting links. Reports online show malicious people disrupt the meetings by sharing threats, posting pornographic images and other such unpleasant messages forcing hosts to shut down their meetings. The top tips to avoid ZoomBombing include the following:

- Avoid publicly sharing meeting links on social media
- Avoid using Zoom Personal Meeting ID (PMI) to host events
- Use the 'Waiting Room' feature to vet and allow participants join a meeting
- Allow participants log into Zoom with an email through which they were specifically invited to the event
- Lock the meeting once all invited participants have joined

Find more details here on how to keep your Zoom meetings safe > https://blog.zoom.us/wordpress/2020/03/20/keep-the-party-crashers-from-crashing-your-zoom-event/