UNIVERSITY OF BIRMINGHAM

Guidance – Zoom

Background

Zoom has been adopted as a videoconferencing tool by the university in addition to our standard tools Microsoft Teams, part of the Office 365 service offering, and Skype or Skype for Business. Many at the university have been using Zoom for some time and there is a tangible financial benefit in acquiring a site licence. It scores highly on usability and functionality and offers a valuable service, particularly for home working during the Covid-19 pandemic, while Office 365 and Teams have not been rolled-out yet to the whole university and Skype, which is nearing end of life, is showing its age.

While Zoom has high usability, it is limited in the area of data protection and security with a number of shortcomings as have been reported in the press. The company has recognized these and has prioritized resolving them.

Reported Issues

- Uninvited visitors may gatecrash meetings if certain basic precautions are not taken; this is known as 'Zoom-Bombing'.
- Meetings can be recorded, and the content accessed by Zoom admin staff, ostensibly for 'training purposes'.
- A large number of Zoom sites have been set up by hackers and used to try to lure unsuspecting or the meeting recorded without the participants knowledge.
- There has been a large increase in Zoom-related phishing attacks via email and social networks seeking to steal user credentials or URLs for meetings or lure them into using fake sites.

Good Practice

Before the meeting

1. Familiarise yourself with the security features-how to remove participants, or put them on hold, or mute them, how to disable file share and screen share, so only the host can share images, powerpoint etc. and control recordings, so others can't record
2. Always set meetings to 'private' not 'public'. This ensures that anyone not invited by the host cannot join the meeting. If you do want to hold a meeting where unknown individuals can join, you MUST disable 'screen and file sharing', 'private chat', and 'screen annotations' and operate with 'mute all' ON. This will allow you to control who contributes to the discussion and prevent inappropriate behaviour.
3. Set up a strong meeting password for all meetings and ensure that unique meeting IDs are generated automatically to reduce the risk of uninvited visitors.
4. Use the "Waiting "Room" feature to have participants wait until the host arrives and vet participants prior to entering the meeting.
5. Limit screen-sharing ability to the host, using the host controls at the bottom of the screen.
6. Turn off file transfer, in-meeting file transfer allows people to share files through the in-meeting chat. Toggle this off to keep the chat from getting bombarded with unsolicited pics, GIFs, memes and other content.
7. Don't use social media to share meeting links as malicious groups can trawl sites for such links.

During the meeting

8. Use the waiting room facility, so you can vet who joins the meeting.
9. Switch off 'call recording' by default, those who require call recording for a legitimate purpose, such as researchers wanting to record interviews, should enable it explicitly together with a pop-up notice to inform all participants that the meeting is being recorded; this will stay on screen while recording is happening. This does not remove the need for consent for research purposes.

10. If using the locally installed Zoom client software, ensure that security patches and updates are installed, normally this is automatic, but you should not try to switch this off. Otherwise use the web version.
11. Avoid sharing documents during a meeting – Zoom stores files in the US – or ensure that files are deleted at the end of the meeting or shortly thereafter.

Conclusion

Zoom is highly functional and is perhaps more intuitive than some competitor services. Its security and privacy shortcomings are being resolved by the company, and with appropriate care it is a tool that will be very useful during and after the current crisis. Therefore, we recommend its use where Teams or Skype are unsuitable or not available, however users should be aware of the issues and take a few basic precautions to ensure that we work as securely as possible. See the table below for help on Zoom configuration settings.

Help on Zoom Configuration Settings[1]

The functions referred-to in the table should be available to meeting organisers, administrators should set the appropriate defaults.

Function	Action	Rationale	Zoom Support
File transfer	Turn off and lock	Risk of accidentally sharing confidential information.	https://support.zoom.us/hc/en-us/articles/209605493
Local recording Cloud recording Automatic recording	Turn off and lock	Recording is only appropriate under certain circumstances. (contact Legal Services for advice on when recording may be permissible)	https://support.zoom.us/hc/en-us/articles/201362473
Private chat	Turn off and lock	Could be saved and viewed by others, therefore not private.	https://support.zoom.us/hc/en-us/articles/203650445
Auto-saving chat	Turn off and lock	Autosaved to the cloud.	https://support.zoom.us/hc/en-us/articles/203650445

Useful guidance

Zoom on security

https://zoom.us/docs/en-us/privacy-and-security.html?zcid=3747&creative=431306240822&keyword=zoom%20security&matchtype=e&network=g&device=c&gclid=EAIaIQobChMI-KChyej86AIVFeDtCh1cOwzkEAAYASAAEgJjLPD_BwE

Zoom on how to keep meetings private

https://blog.zoom.us/wordpress/2020/03/20/keep-uninvited-guests-out-of-your-zoom-event/

Zoom's approach

https://blog.zoom.us/wordpress/2020/04/01/a-message-to-our-users/

National Cyber Security Centre advice on teleconferencing services

https://www.ncsc.gov.uk/guidance/video-conferencing-services-security-guidance-organisations

[1] Courtesy of University of Oxford, Medical Sciences Division