Zoom Safety in IAP2 Meetings and Training

Contents

Introduction

IAP2 Australasia have chosen to use Zoom as our "virtual meeting room" platform for our training, meetings and events. In fact, IAP2 Australasia has used Zoom for several years now for many of our activities, due to the geographical spread of our Directors, Trainers, team members, working groups and participants across Australia and New Zealand.

Like you, we have heard in the news the security concerns being raised surrounding the use of Zoom – such as unwanted guests crashing meetings with unwanted content.

Of course, we value the security of our participants, and so IAP2 Australasia, in light of these reports, have researched the safety of using Zoom.

Here we share what we have found and also outline the measures and checklists we have put into place to make our Zoom meeting rooms as secure as possible. Our aim is not to make any definitive claims about the safety of Zoom, but to help provide you with information and share what we have found.

We will continue to keep up to date with the various measures that Zoom is taking to tighten up the security of the platform, and have collated a list of links and releases from Zoom which address various concerns that you, or your IT department, may have.

What are the security issues, and why do they happen?

The number of daily users of Zoom exploded from 10 million to 200 million from December to March, and many reports of trolls crashing meetings and flashing unwanted content emerged. There were also reports of leaked emails and bugs that may have allowed hackers to access webcams, and that Zoom was sharing information with third parties.

It would appear that many of the security issues publicised lately has been caused by security features of Zoom (such as password access) not being put in place by the meeting organiser.

For example, a lot of the press around "Zoom Bombing" is occurring where users hadn't secured their meeting rooms correctly and made them publicly available to join.

From what we can see, Zoom have responded quickly to continue the upgrade of security, putting all other development on hold. Zoom have been publishing security upgrades over the last few weeks and are continuing to do so. Regular users of Zoom will have noticed these updates with fixes happening over recent weeks.

Before using Zoom

The first thing to do, before each Zoom meeting, is to make sure you are using the latest version of Zoom which will include the current security fixes.

You can do this by:

- Using the online browser based Zoom platform OR
- Follow this link to update the Zoom app already installed on your computer, tablet or smartphone https://support.zoom.us/hc/en-us/articles/201362233-Where-Do-I-Download-The-Latest-Version-

What IAP2 Australasia is doing

Here at IAP2A we have been reviewing all the settings for our own Zoom account and have implemented all the security features available to minimise security issues for all of our meetings, trainings and events.

IAP2 staff, who are responsible for hosting our online events, follow a checklist of settings and processes to maximise security for our meetings and participants.

In particular, our Zoom meetings will have the following in place, to minimise any potential problems:

- IAP2A meetings and trainings will be password protected to stop Zoom-bombing opportunities,
- Only registered participants or invited guests will be admitted into meetings and trainings,
- Meetings will be locked once all participants have been admitted to stop unauthorised access.

For more information, feel free to contact IAP2 Australasia at info@iap2.org.au.

You may also find the links below helpful as these outline how Zoom has been addressing security concerns and applying fixes as these concerns arise.

Links and further reading

IMPORTANT UPDATE TO ZOOM ADMINS: 29 APRIL 2020

On May 30th, 2020, Zoom will enable GCM encryption across the entire Zoom platform, providing increased protection for meeting data. After May 30, 2020, all Zoom clients on older versions will receive a forced upgrade when trying to join meetings as GCM Encryption will be fully enabled across the Zoom platform. Please begin updating all your clients to Zoom 5.0 now. Zoom admins, visit our 5.0 IT administrator page for more detailed instructions on updating your endpoints to ensure they will be able to support GCM encryption once we cutover on May 30.

Zoom Encryption

As at 1 April 2020, Zoom advised that they have corrected the issue with Windows and Zoom that introduced a potential security fault: https://blog.zoom.us/wordpress/2020/04/01/facts-around-zoom-encryption-for-meetings-webinars/

Where to Download the Latest Version of Zoom

https://support.zoom.us/hc/en-us/articles/201362233-Where-Do-I-Download-The-Latest-Version-

Zoom's Security Page

https://zoom.us/docs/en-us/privacy-and-security.html

How to Avoid Zoom Bombing

https://blog.zoom.us/wordpress/2020/03/20/keep-the-party-crashers-from-crashing-your-zoom-event/

Other Zoom Links:

- https://blog.zoom.us/wordpress/2020/04/01/a-message-to-our-users/
- https://blog.zoom.us/wordpress/2020/04/01/facts-around-zoom-encryption-for-meetings-webinars/
- https://blog.zoom.us/wordpress/2020/04/08/zoom-product-updates-new-security-toolbar-icon-for-hosts-meeting-id-hidden/

For a more detailed overview of Zoom's security policies, please refer to Zoom's 'Security White Paper' available to download here: https://zoom.us/docs/doc/Zoom-Security-White-Paper.pdf

10 Things You Can Do To Secure Zoom Meetings

The following information, published by tech news site, ZDNet, may also be helpful if you are running your own Zoom meetings:

1. PASSWORD PROTECT YOUR MEETINGS

The simplest way to prevent unwanted attendees and hijacking is to set a password for your meeting. Passwords can be set at the individual meeting, user, group, or account level for all sessions. In order to do so, first sign in with your account at the Zoom web portal. If you want to set up a password at the individual meeting level, head straight over to the "Settings" tab and enable "Require a password when scheduling new meetings", which will ensure a password will be generated when a meeting is scheduled. All participants require the password to join the meeting. Subscription holders can also choose to go into "Group Management" to require that everyone follows the same password practices.

2. AUTHENTICATE USERS

When creating a new event, you should choose to only allow signed-in users to participate.

3. JOIN BEFORE HOST

Do not allow others to join a meeting before you, as the host, have arrived. You can enforce this setting for a group under "Account Settings."

4. LOCK DOWN YOUR MEETING

Once a session has begun, head over to the "Manage Participants" tab, click "More," and choose to "lock" your meeting as soon as every expected participant has arrived. This will prevent others from joining even if meeting IDs or access details have been leaked.

5. TURN OFF PARTICIPANT SCREEN SHARING

No-one wants to see pornographic material shared by a Zoom bomber, and so disabling the ability for meeting attendees to share their screens is worthwhile. This option can be accessed from the new "Security" tab in active sessions.

6. USE A RANDOMLY-GENERATED ID

You should not use your personal meeting ID if possible, as this could pave the way for pranksters or attackers that know it to disrupt online sessions. Instead, choose a randomly generated ID for meetings when creating a new event. In addition, you should not share your personal ID publicly.

7. USE WAITING ROOMS

The Waiting Room feature is a way to screen participants before they are allowed to enter a meeting. While legitimately useful for purposes including interviews or virtual office hours, this also gives hosts greater control over session security.

8. AVOID FILE SHARING

Be careful with the file-sharing feature of meetings, especially if users that you don't recognize are sending content across, as it may be malicious. Instead, share material using a trusted service such as Box or Google Drive. At the time of writing, Zoom has disabled this feature anyway due to a "potential security vulnerability."

9. REMOVE NUISANCE ATTENDEES

If you find that someone is disrupting a meeting, you can kick them out under the "Participants" tab. Hover over the name, click "More," and remove them. You can also make sure they cannot rejoin by disabling "Allow Removed Participants to Rejoin" under the "Settings: Meetings - Basic" tab.

10. CHECK FOR UPDATES

As security issues crop up and patches are deployed or functions are disabled, you should make sure you have the latest build. In order to check, open the desktop application, click on your profile in the top-right, and select "Check for updates."

Reference:

https://www.zdnet.com/article/make-sure-your-zoom-meetings-are-safe-by-doing-these-10-things/

https://www.latimes.com/business/technology/story/2020-04-13/is-zoom-safe-to-use-heres-what-you-need-to-know