Zoom Security & Best Practices

Updated: August 23, 2021

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 can choose to only allow signed-in users to participate.

3. Require Registration

Instead of sharing the link to a Zoom meeting or Zoom webinar, require registration. A link to a registration screen requires prospective attendees to submit their name, a valid email and, optionally, we can provide a comments field if they wish to supply questions for the session. After submitting, an email goes to the inbox of the account they specified. This link only works for one connection and cannot be shared with a crowd of people intending to zoom bomb.

4. Disable 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." For normal daytime meetings that are not public meetings, Join before Host is very convenient. For afterhours, public events this option is highly discouraged.

5. 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. This is good for classes and non-public-meetings.

6. Turn off participant screen sharing

No-one wants to see offending material shared by a Zoom bomber. 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.

7. 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.

8. 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.

9. 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."

10. 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.

11. 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."

12. Scheduling

If you use the mobile Zoom app on your smart phone, and open meetings, you will only see single event meetings listed chronologically. If you swipe down to the bottom you will find all the recurring meetings listed separately and quite inconveniently.

I strongly recommend not using the mobile app to schedule meetings and instead use the web portal. The potential for double booking because of this poor programming decision can be awkward and catastrophic.

13. Closed Captioning

Zoom now supports closed captioning and the quality of the transcription is very good. Many people have requested closed captioning for their Zoom sessions since we started using the software last March. Initially, Zoom did not support built-in CC with t heir software but did allow 3rd party plug-ins to do the job at an additional cost. Our work around for this need was to purchase a few licenses of otter.ai – more of a transcription service with additional features, it met most of our needs but was inconvenient for some in practice and costs us money.

In your Zoom sessions click on the Live Transcript option in the bottom menu and then select **ENABLE Auto-Transcription** it is a toggle between enable and disable.

14. Recording

Not all meetings need to be recorded. Public meetings certainly can and should. Job interviews and personnel matters probably not. Hosts and co-hosts can start and stop recordings and should be aware at the outset whether or not a meeting should be recorded and to enable pressing the record button if it is not enabled rom setup.