PROTECTING YOURSELF AND OTHERS ON ZOOM

29 March 2020

Zoom is a good online meeting & conferencing tool but with any collaboration tool comes risks for the unwary. There are options to protect yourself and others from people misusing Zoom.

'**Zoombombing**' is now a thing with people jumping into online meetings/classes then sending porn and other images to all in a call. Or perhaps listening in to things they should not be.

It's possible someone could infiltrate a meeting and send an infected document (Word, Excel or PowerPoint). While there's been no reports, it's only a matter of time before it happens. There's a Zoom option to limit the types of files transferred during an online meeting, see below.

Unlike some other online collaboration, there's no content moderation possible. It's all happening in real time.

Open Defaults

The core problem is that some Zoom settings allow a lot of access and that opens opportunities for horrible people.

It's an overall problem in common with many services. The systems are designed for ease of use, less support and fewer complaints.

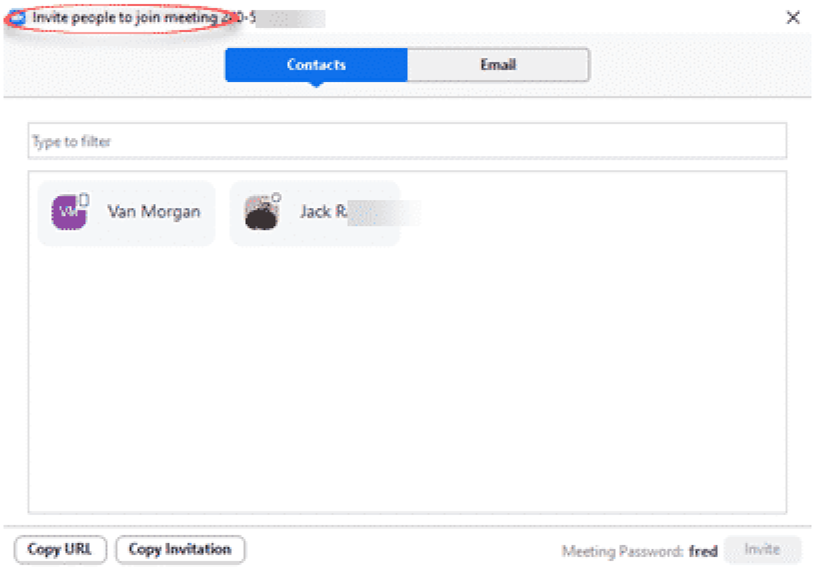
That openness and easy start has made Zoom very popular but left people vulnerable.

Here's some suggestions to limit the risk of unwanted intrusions in your Zoom call.

Limit participants to Zoom meetings

Invite specific people into an online call, conference or class. Don't have a general meeting code/invitation that anyone can use.

Let all participants know the meeting time and ask them to be ready with their Zoom app open. Start the call without a personal meeting ID then invite people into the class from your Zoom contacts list. Each invitee will see a pop-up invitation in their Zoom app.



Meeting Password: fred

There are options to Copy URL or Copy Invitation to let others into the online meeting.

Individual invitations are clumsy, especially if you're dealing with ten or more people, like an online classroom. But it's the best way to prevent unwanted participants. *(It's similar to sharing file/documents options in Office and OneDrive. Instead of making a link available to anyone, specifically nominate the people who can access the file).*

Ideally don't issue a general invitation with a single meeting code. That's easier but allows other people access to the call if they get the code. If you must use a meeting code, share it confidentially via emails or better, instant messaging. Ask participants NOT to share the code with others.

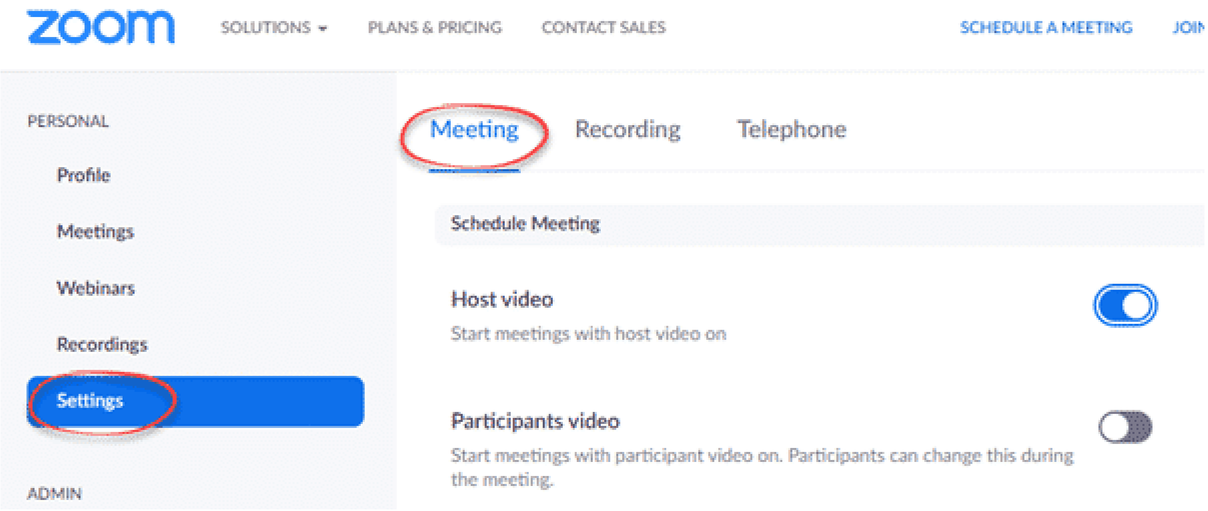
Settings to change

Here's some default settings in Zoom that should be changed to stop people Zoombombing a meeting with unwanted images, videos or files.

Limit Screen Sharing

Screen Sharing should be limited to the host only. The default is to allow anyone to share their screen.

These settings are changed in your Zoom account online NOT in the apps (it varies between platforms but all the setting are online at Settings | Meetings.



Host video

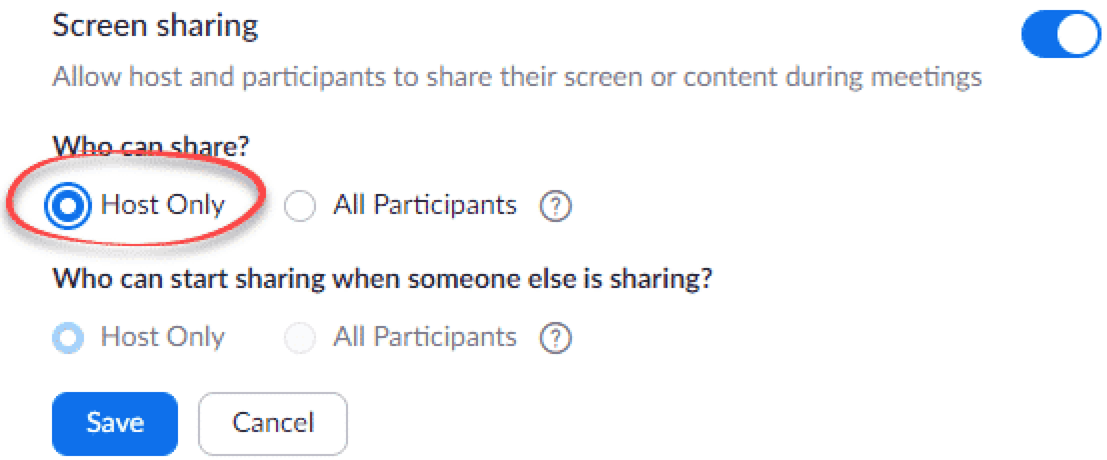
Start meetings with host video on

Participants video

Start meetings with participant video on. Participants can change this during the meeting.

(Note we've turned Host video on but Participants video off by default. Leaving video off decreases bandwidth use and reduces the risk of dropouts).

Scroll way down to the **In Meeting** section then even further down to Screen Sharing. If you wish, turn screen sharing off. More likely you'll want screen sharing (it's really useful) but need to limit access.



Screen sharing

Allow host and participants to share their screen or content during meetings

Who can share?

● Host Only ○ All Participants ?

Who can start sharing when someone else is sharing?

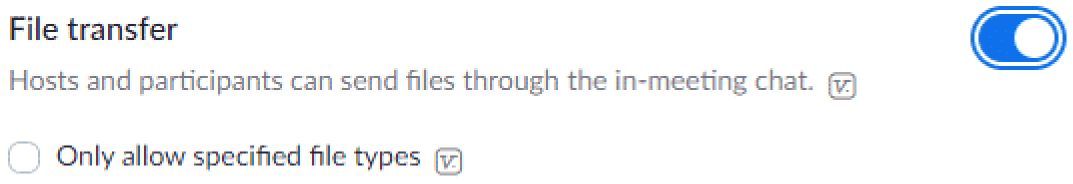
● Host Only ○ All Participants ?

Who can share – Host only
Who can start sharing when someone else is sharing — Only Host (this option isn't available if 'Only Host' can share)

File Transfer OFF

File Transfer are also very useful but a possible risk. An intruder could send awful images or videos plus the risk of sending virus infected documents.

Turn File transfer off, if you're sure you won't need it at Settings | Meetings | In meeting settings. Otherwise limit what can be transferred.



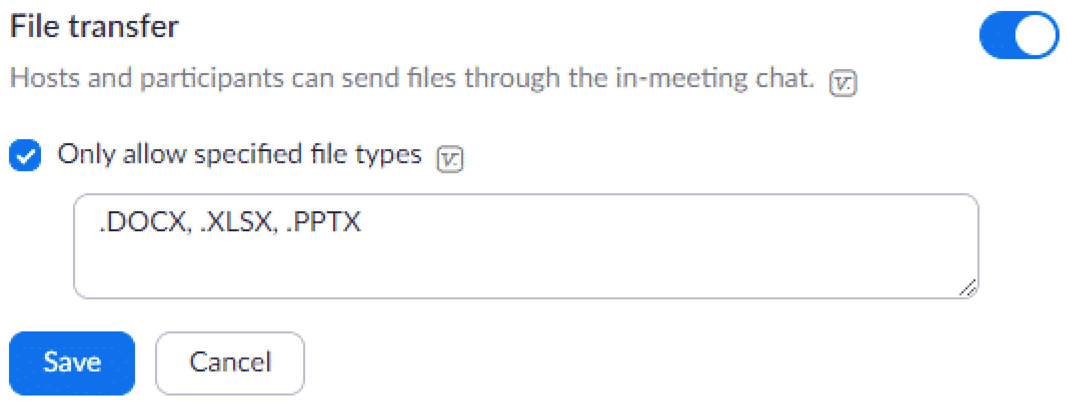
File transfer

Hosts and participants can send files through the in-meeting chat.

☐ Only allow specified file types

Limit File Transfers

Or limit file transfers to certain file types such as the main Office document types:



File transfer

Hosts and participants can send files through the in-meeting chat.

☑ Only allow specified file types

.DOCX, .XLSX, .PPTX

Only allow specified file types – ON

The file types are separated by commas with a dot/period prefix.

.DOCX , .XLSX , .PPTX

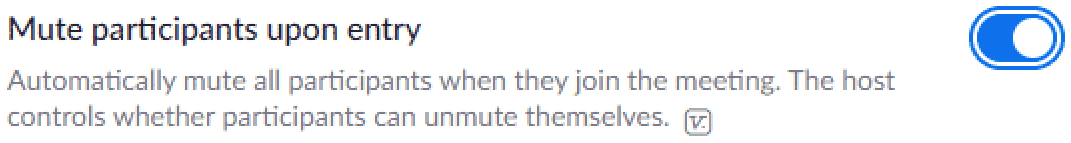
You might want to add images like .JPG or .PNG

Entry / Exit controls

Some other options worth considering to monitor who is entering or leaving a Zoom meeting.

Mute participants upon entry

This lets the Zoom meeting host control who can be heard in the online meeting. It defaults OFF.

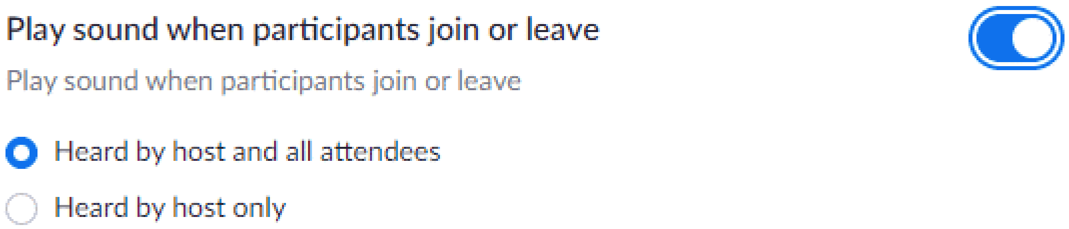


Mute participants upon entry

Automatically mute all participants when they join the meeting. The host controls whether participants can unmute themselves.

Play sound when participants join or leave a Zoom meeting

A simple way to keep track of who is in or out of the meeting. Hopefully you'll quickly notice if there's unwanted meeting participants.



Play sound when participants join or leave

Play sound when participants join or leave

● Heard by host and all attendees

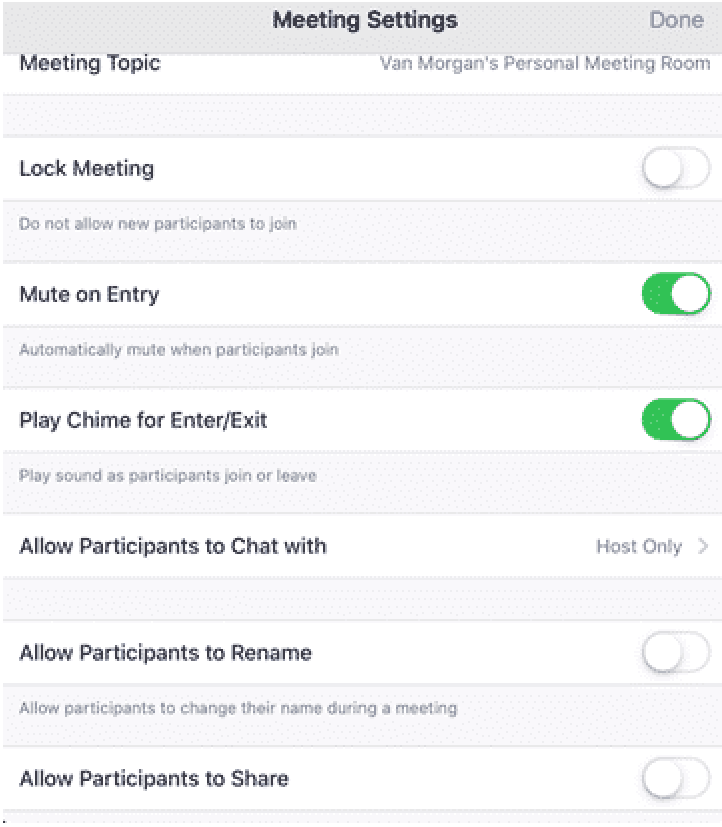
○ Heard by host only

Play sound when participants join or leave

- Heard by host and all attendees
- Heard by host only

iPad Meeting Settings

On the Zoom iPad app, the options are under the More button at top left of a Meeting, then Meeting Settings:



Meeting Settings Done

Meeting Topic Van Morgan's Personal Meeting Room

Lock Meeting ○

Do not allow new participants to join

Mute on Entry ●

Automatically mute when participants join

Play Chime for Enter/Exit ●

Play sound as participants join or leave

Allow Participants to Chat with Host Only >

Allow Participants to Rename ○

Allow participants to change their name during a meeting

Allow Participants to Share ○

The above image shows recommended settings:

Mute on Entry – ON
Play chime on Enter/Exit – ON
Allow Participants to Chat with – Host Only (this isn't always wanted, be aware there are options to limit text chat in a meeting)
Allow Participants to Rename – an unwanted 'guest' could rename to disguise themselves. Though they can still change their name before joining the meeting.
Allow Participants to Share – OFF

Source: https://office-watch.com/2020/protecting-yourself-and-others-on-zoom/