SECUREMISR
A CYSIV COMPANY

SECURITY ADVISORY
Securing your Online Zoom Meetings

April 19, 2020

The COVID-19 virus outbreak forced millions of people around the world to work from home as part of the enforced social distancing policy to help stop the virus's spread. As a result, workers turned to video conferencing platforms like Zoom to ensure business continuity and to stay connected.

If you found yourself responsible for hosting an online meeting to connect with your remote workers, your class students or your webinar attendees, then here are some useful tips to keep it secure and keep unwanted intruders away but first, keep these Zoom basics in mind:

- **Anyone with the meeting link can join your meeting**. When you share your meeting link on social media or other open forums, it makes your event public for anyone to join.
- **Anyone can join unprotected meetings if they have the Meeting ID**. Even if they don't have the meeting link, if someone knows – or successfully guesses - your meeting ID, then they can join and eavesdrop on your meeting. This is called Zoom-bombing.

Since the last surge in the number of daily users on Zoom from 10 million last December to more than 200 million today[1], many attacks have been reported to target unprotected zoom meetings. Some attackers would hijack meetings and eavesdrop on their chats while others

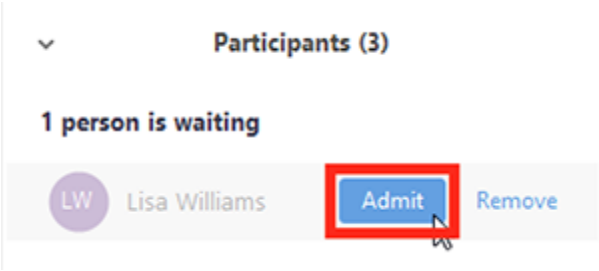
posted inappropriate content and hate language in classroom meetings and public events. To keep your Zoom meeting safe from unwelcome intruders, consider enabling the following features when hosting your next Zoom meeting:

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

- **Always protect your meetings with passwords.**[2] Tools exist that brute-forces meeting-ids, allowing intruders to get into meetings and do everything from eavesdropping to posting inappropriate content. Zoom has fixed this issue by setting a password by default to all new meetings.
- **Don't use your Personal Meeting ID (PMI) to host public events:** Your Personal Meeting Room is a virtual meeting room permanently reserved for you and accessible with your (PMI). Because it is always accessible with the same Meeting ID and personal link, it should not be used for meetings with participants you do not meet regularly because once a participant has the link to your PMI, they can join at any time when the meeting is in use. It is ideal to only use is it with participants you meet with regularly.
- **Always keep your Zoom updated with the latest version**. New patches are released regularly to fix security vulnerabilities in Zoom. Updating makes sure your device is safe and you enjoy the latest features like auto password-protecting meetings. This is especially important in the coming days, where more security issues are expected to emerge and get patched because of the huge spike in Zoom number of users.
- **Limit access to meeting link**[3]**:** Send your meeting invitation link selectively by SMS, Email or IM applications. Sharing your meeting link on public platforms like Facebook and Twitter makes it susceptible to intruders. If hosting a public event, ask attendees first to register their email addresses using services like Google forms or Eventbrite, then send the meeting link and password privately to them.
- **Allow only signed-in users to join:** If someone tries to join your event and isn't logged into Zoom with the email they were invited through, they will not be let in. This is useful if you want to make sure only invited participants can join.
- **Waiting room:** This is a great option to make sure you recognize everyone in the meeting. It allows you to only let invited guests into your event. When enabled, all guests will need your explicit **admission** before joining your meeting, even if they have the

[2] https://www.fbi.gov/contact-us/field-offices/boston/news/press-releases/fbi-warns-of-teleconferencing-and-online-classroom-hijacking-during-covid-19-pandemic
[3] https://zoom.us/docs/doc/Zoom-Security-White-Paper.pdf

correct link and password. This way, you have the chance to have a brief look at every guest before letting them in. If you don't recognize someone, you can simply **Remove** them from the meeting.

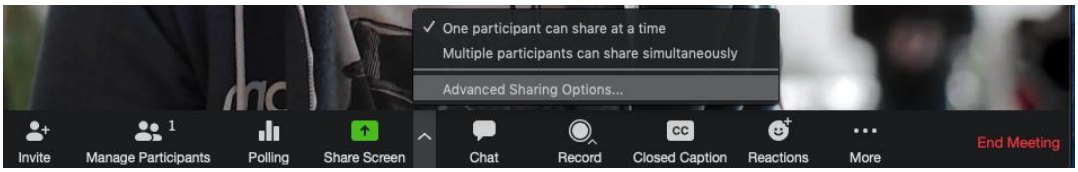


- **Remove unwanted or disruptive participants:** From that Participants menu, you can mouse over a participant's name where several options will appear, including Remove. Click that to exclude an attendee from the meeting. They won't be able to rejoin unless you allow participants and panelists to rejoin.
- **Lock the meeting:** When you lock a Zoom Meeting that's already started, no new participants can join, even if they have the meeting ID and password. Do this when everyone has joined the meeting to make sure no unwelcome guests interrupt your calls. In the meeting, click Participants at the bottom of your Zoom window. In the Participants pop-up, click the button that says Lock Meeting.

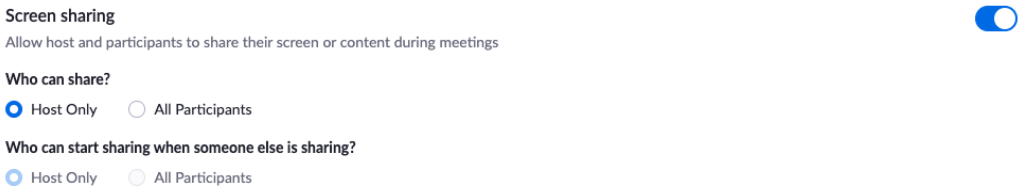
The above security capabilities ensure that meetings are only attended by invited participants. To better manage your meetings and avoid any non-productive contributions from attendees while the meeting is running, Zoom offers more useful controls:

- **Manage screen sharing:** You do not want random participants in your public event taking control of the screen and sharing unwanted content with the group. You can restrict this — before the meeting and during the meeting in the host control bar — so that you're the only one who can screen-share.

  To prevent participants from screen sharing during a call, using the host controls at the bottom, click the arrow next to Share Screen and then Advanced Sharing Options.



Under “Who can share?” choose “Only Host” and close the window. You can also lock the Screen Share by default for all your meetings in your web settings.



- **Put attendee on hold:** Just like sending them to waiting rooms, Attendee On Hold allows the host to stop video and audio transmission to a participant. This allows others to continue the meeting while temporarily preventing any participants who are on hold from seeing and hearing the other participants. To activate this feature, click on someone’s video thumbnail and select Start Attendee on Hold. Click Take Off Hold in the Participants list when you’re ready to have them back.
- **Disable video:** Hosts can turn someone’s video off. This will allow hosts to block unwanted, distracting, or inappropriate gestures on the meeting screen.
- **Mute participants:** Like the video, hosts can disable the microphone of individual participants or all of them at once. Hosts can block unwanted, distracting, or inappropriate noise from other participants. You can also enable Mute Upon Entry in your settings to stop new users from disrupting your meeting when joining.
- **Turn off annotation:** You and your attendees can doodle and mark up content together using annotations during a screen share. You can disable the annotation feature in your Zoom settings to prevent participants from writing all over the screens.
- **Disable private chat:** Zoom has in-meeting chat for everyone or participants can message each other privately. Restrict participants’ ability to chat amongst one another while your event is going on and cut back on distractions. This is really to prevent anyone from getting unwanted messages during the meeting.

References:

1. https://blog.zoom.us/wordpress/2020/03/20/keep-uninvited-guests-out-of-your-zoom-event/
2. https://zoom.us/docs/doc/Zoom-Security-White-Paper.pdf
3. https://www.fbi.gov/contact-us/field-offices/boston/news/press-releases/fbi-warns-of-teleconferencing-and-online-classroom-hijacking-during-covid-19-pandemic