KANSAS ASSOCIATION OF COUNTIES

ZOOM MEETING PROTECTION

The rapid spread of COVID-19 forced a vast majority of employers and governments to transition its operations to some sort of online platform. Most of these organizations use one specific virtual teleconference platform, Zoom, to virtually host meetings and conduct business. Unfortunately, with this online platform use comes an increase in cyber-hacking; the most recent form coming as unauthorized drop-ins on Zoom meetings, also known as "Zoombombing". Zoom bombers commandeer meetings and bombard the screen with inappropriate at best content. Reports of vulgar, hateful content appearing on screens combined with uninvited participants discussing a range of topics continue to flood into Zoom and the FBI's cyber-attack division. As such, multiple sources publish tips and tricks to protect a Zoom meeting from an unwanted Zoom-bomber.
KAC collected and combined those tips into one reference sheet below:

BEFORE BEGINNING A MEETING:

UPDATE YOUR ZOOM APPLICATION:

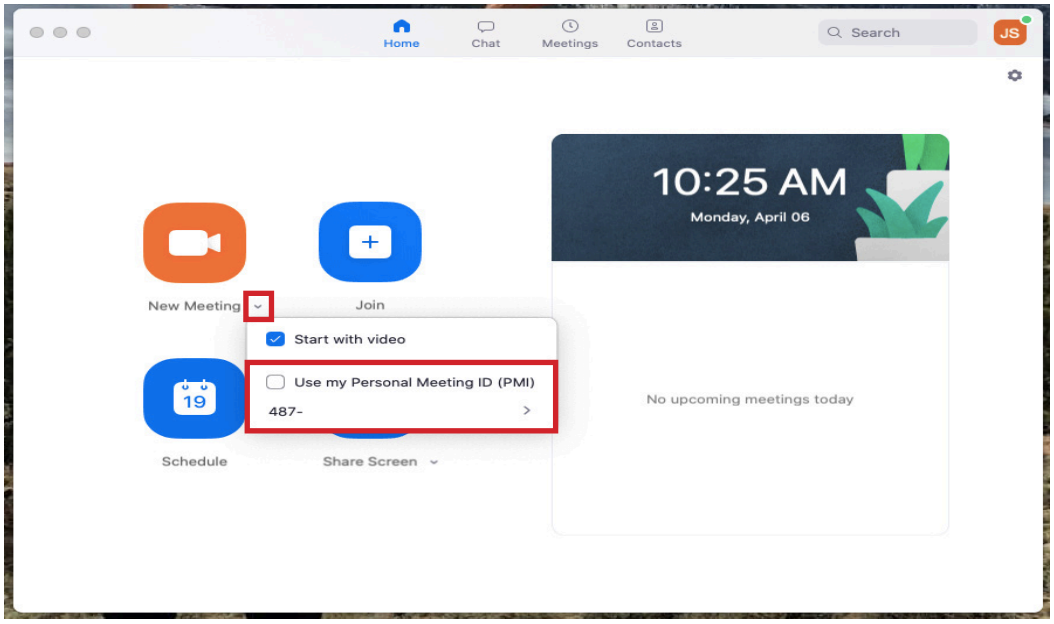
Zoom as a company constantly works to implement security features and extend privacy to its users. However, those continuous implementations only work if users frequently update the application. While the application notifies you of updates available, checking for updates regularly ensures you're using the most up to date (and typically, the most protective) version of the app.

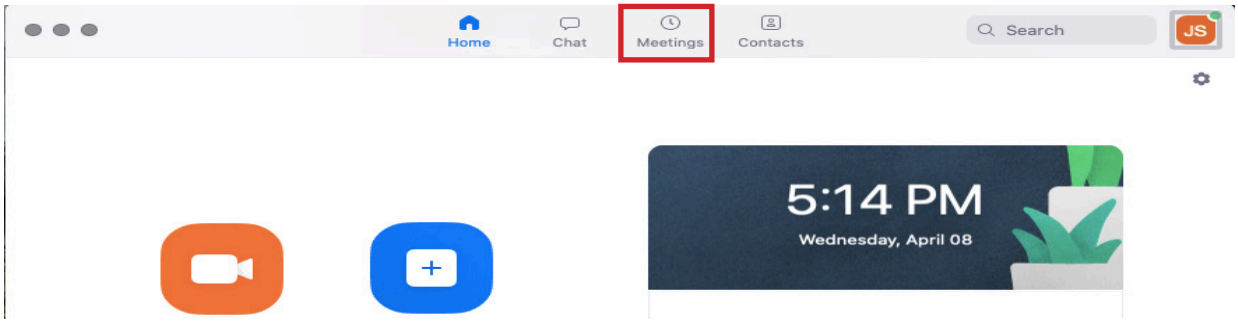
USE A RANDOM MEETING ID INSTEAD OF YOUR PERSONAL MEETING ID:

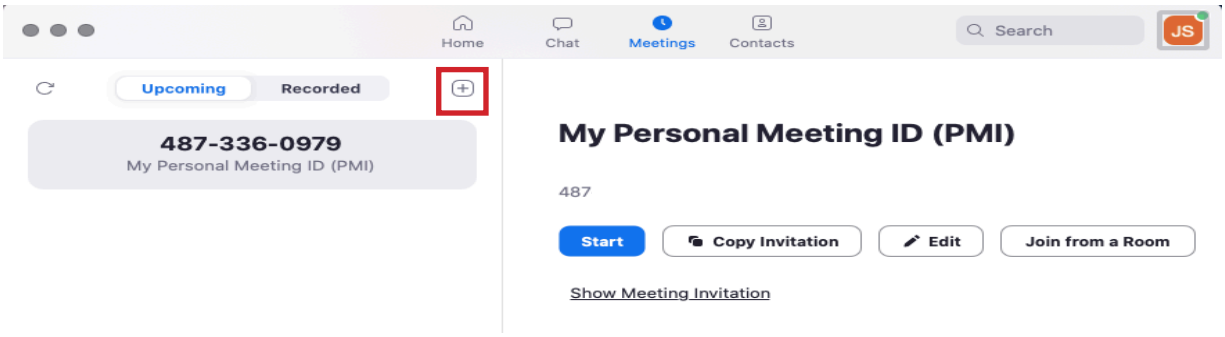
Zoom allows you to host meetings under a randomly assigned meeting ID instead of your personal meeting ID. This function protects your hardware and private information from unauthorized access.

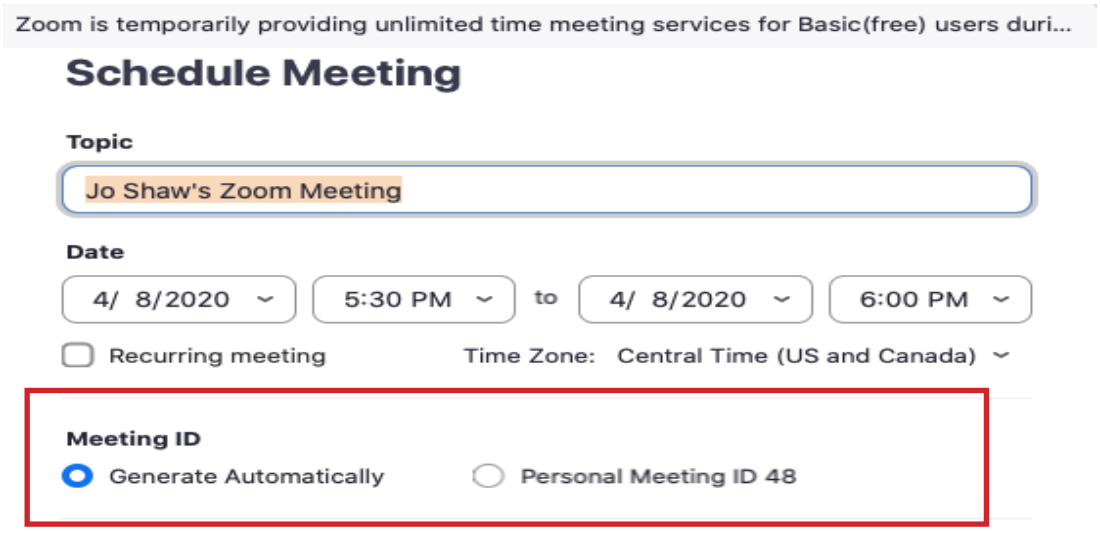
When setting up a meeting, there's two ways to set up use of a random meeting ID:

- On the "Home" page, select the arrow next to the "New Meeting" button. Ensure the box next to "Use my Personal Meeting ID" is unchecked.
- On the "Meetings" page, select the "+" box to the right of the "Recorded" button just right of center at the top of the page.
- This opens a "Schedule Meeting" window.
- Under "Meeting ID" ensure the "Generate Automatically" button is selected (This method ensures a random ID at every meeting, including a recurring meeting scheduled.)
- Avoid using the "Start" button under the PMI section of the "Meetings" page.


Home
Chat
Meetings
Contacts
Search
JS
10:25 AM
Monday, April 06
New Meeting
Join
Start with video
Use my Personal Meeting ID (PMI)
487-
Schedule
Share Screen
No upcoming meetings today


Home
Chat
Meetings
Contacts
Search
JS
5:14 PM
Wednesday, April 08

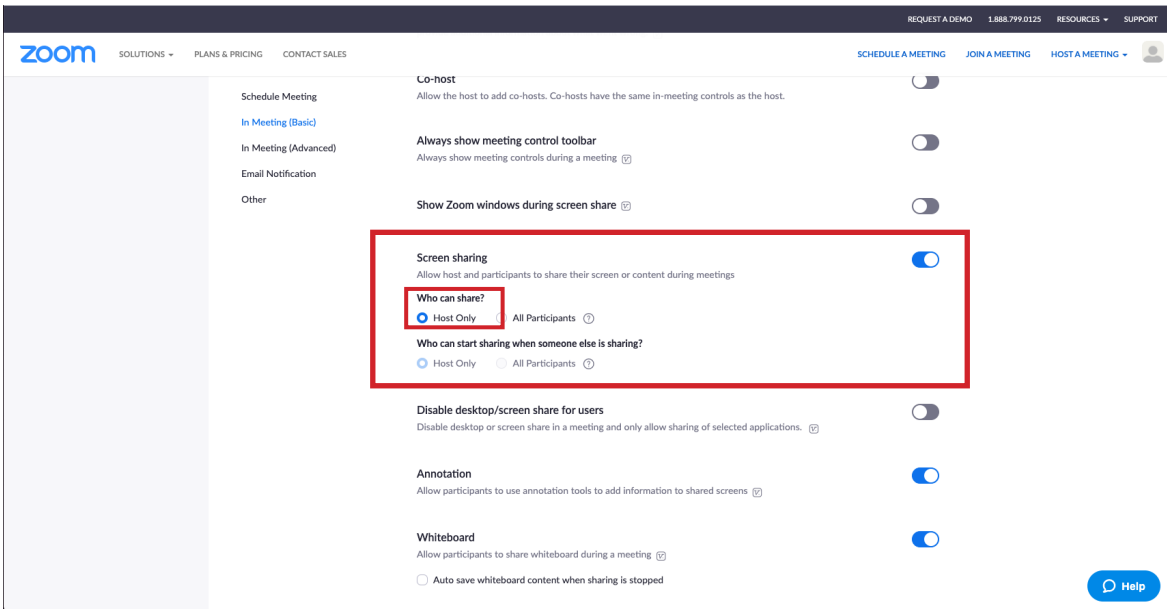

Home
Chat
Meetings
Contacts
Search
JS
Upcoming
Recorded
487-336-0979
My Personal Meeting ID (PMI)
My Personal Meeting ID (PMI)
487
Start
Copy Invitation
Edit
Join from a Room
Show Meeting Invitation


Zoom is temporarily providing unlimited time meeting services for Basic(free) users duri...
Schedule Meeting
Topic
Jo Shaw's Zoom Meeting
Date
4/ 8/2020
5:30 PM
to
4/ 8/2020
6:00 PM
Recurring meeting
Time Zone: Central Time (US and Canada)
Meeting ID
Generate Automatically
Personal Meeting ID 48

DISABLE SCREEN SHARING FOR PARTICIPANTS:

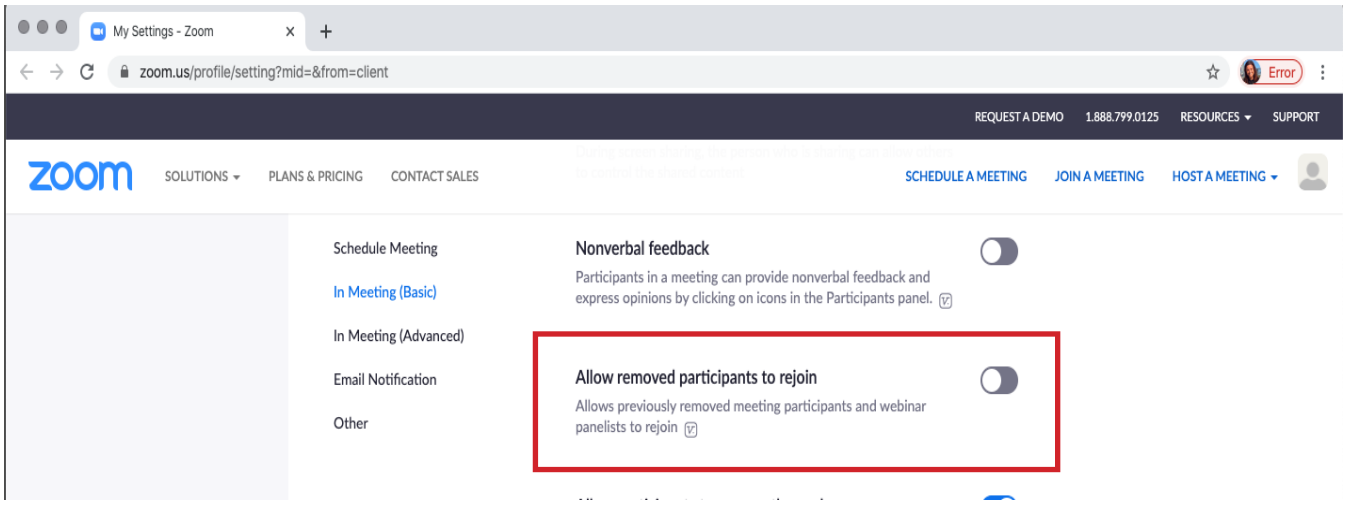
Zoom features a screen sharing function that allows participants of a meeting to share what's on their screen in order to enhance a presentation.

- Select the settings button, the cog wheel on the top right corner the zoom "Home" page.
- Select "View More Settings" – this will open a webpage prompting you to log in to your Zoom account.
- Once logged in, select "Settings" from the menu on the left-hand side. This brings up every setting regarding a Zoom meeting on your account.
- Under the "In Meeting (Basic)" section, scroll down to "Screen Sharing". Ensure that the "Host Only" button is selected, disabling participants from the ability to screen share.
- This setting can be changed by the host during a meeting by selecting the arrow next to the green "Screen Share" button and enable participants to screen share.



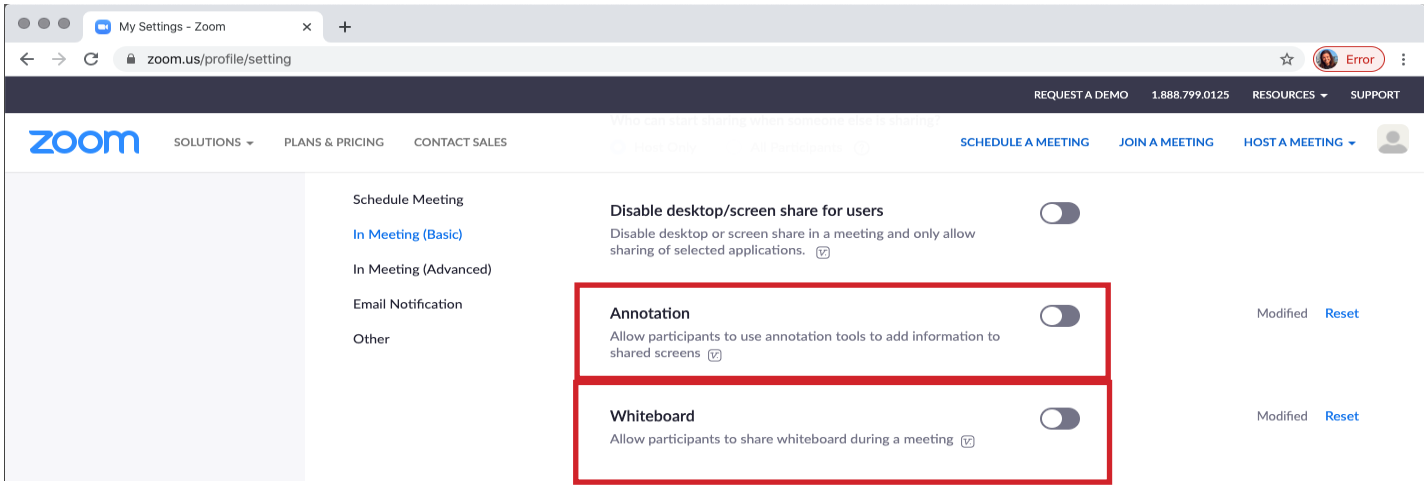
ENSURE REMOVED PARTICIPANTS ARE NOT ABLE TO REJOIN A MEETING:

- Select the settings button, the cog wheel on the top right corner the zoom “Home” page.
- Select “View More Settings” – this will open a webpage prompting you to log in to your Zoom account.
- Once logged in, select “Settings” from the menu on the left-hand side. This brings up every setting regarding a Zoom meeting on your account.
- Under the “In Meeting (Basic)” section, scroll down to “Allow removed participants to rejoin”
- Ensure this section is set to “off” or grey, prohibiting removed participants from rejoining.



DISABLE ANNOTATIONS & WHITEBOARD PRIVILEGES FOR PARTICIPANTS:

- Select the settings button, the cog wheel on the top right corner the zoom “Home” page.
- Select “View More Settings” – this will open a webpage prompting you to log in to your Zoom account.
- Once logged in, select “Settings” from the menu on the left-hand side. This brings up every setting regarding a Zoom meeting on your account.
- Under the “In Meeting (Basic)” section, scroll down to the “Annotation” section and “White Board” section.
- Ensure both sections are set to “off” or grey, prohibiting participants from utilizing these tools.

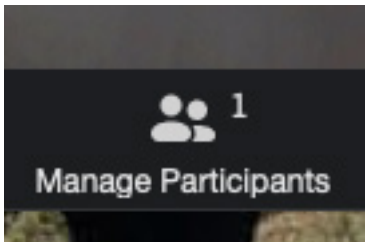


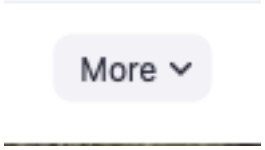
DURING A MEETING:

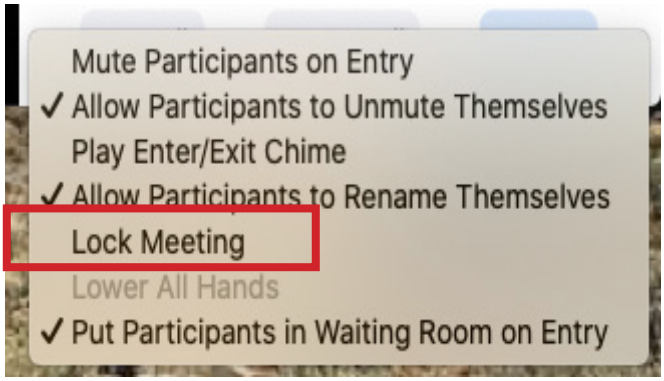
LOCK YOUR MEETING ONCE ALL PARTICIPANTS HAVE ENTERED*:

Once meeting is commenced, the host can lock the meeting to prevent ANY other participants from entering the meeting, including those with an invitation link and password.

- in the meeting, open the "Participants" window. In the "Participants" pop-up, click the "Lock Meeting" button.
- IMPORTANT NOTE: this function locks out ANY participants, including those with proper credentials for entering the meeting. It would be prudent to ensure all those who are invited to the meeting are aware of your intent to lock the meeting after a certain time.







* If your meeting is subjet to the Kansas Open Meetings Act in that you are meeting for the conduct of government affairs or the transaction of governmental business, the meeting must NOT be locked.

Instead, utilize the waiting room feature and disable participants' abilities to annotate, screen share, and whiteboard privilieges to maintain control of your public meeting.