



C U Y A M A C A  
· C O L L E G E ·

## SAFELY SETTING UP ZOOM MEETINGS / EVENTS

1. Avoid sharing your meeting links publicly. Instead, schedule a meeting or event that requires participants to [register](#) with their name and email address.
2. For added security, [require a password](#) that participants must enter before being allowed into a meeting.
3. For public meetings and events, NEVER use your Personal Meeting ID (PMI). Your PMI is set up as one continuous meeting, once someone has a link to your PMI they can enter it any time. Always set up public meetings/events using [random meeting IDs](#).
4. [Enable a Waiting Room](#) so you have control over who can enter your meeting. The [Waiting Room](#) feature gives hosts greater control over session security.
5. Additionally, 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."
6. Mute participants upon entry. Having attendees [muted as they join](#) will reduce ambient noise and minimize disruption.

### Schedule Meeting

#### Topic

#### Date & Time

11/18/2020 to 10:00 AM to 10:30 AM 11/18/2020

Recurring meeting Time Zone: Pacific Time (US and Canada)

#### Meeting ID

Generate Automatically  Personal Meeting ID 786 924 2200

#### Security

- Passcode 523144 Only users who have the invite link or passcode can join the meeting
- Waiting Room Only users admitted by the host can join the meeting

#### Video

Host  On  Off Participants  On  Off

#### Audio

Telephone  Computer audio  Telephone and computer audio  
Dial in from United States [Edit](#)

#### Calendar

iCal  Google Calendar  Outlook  Other Calendars

#### Advanced Options

- Allow participants to join anytime
- Mute participants upon entry
- Only authenticated users can join: Sign in to Zoom
- Request permission to unmute participants
- Automatically record meeting in the cloud

#### Alternative Hosts:

#### Meeting Type:

 (Optional)

#### Interpretation

Enable language interpretation

# SAFETY TIPS DURING ZOOM MEETINGS / EVENTS

## USING CHAT SAFELY

The [chat feature allows varying levels of safety, and they can all be changed during the meeting if you need to make adjustments](#). For events with external (non-Cuyamaca) attendees, it is recommended all chat functions are disabled. Additionally, [the file transfer option should be disabled](#). In addition to the unwanted sharing of information, malware can be shared via a Zoom file transfer.

### File transfer

Hosts and participants can send files through the in-meeting chat. This option cannot be enabled if the End-to-end encryption option is enabled.



## ENABLE SCREEN SHARE FOR “HOST ONLY”

Preventing others from screen sharing will secure your meeting from unwanted and disruptive visuals, videos, etc. Attendees may request permission to share screen, and it can be granted during a meeting, only trusted attendees should be granted this access.

### Screen sharing

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

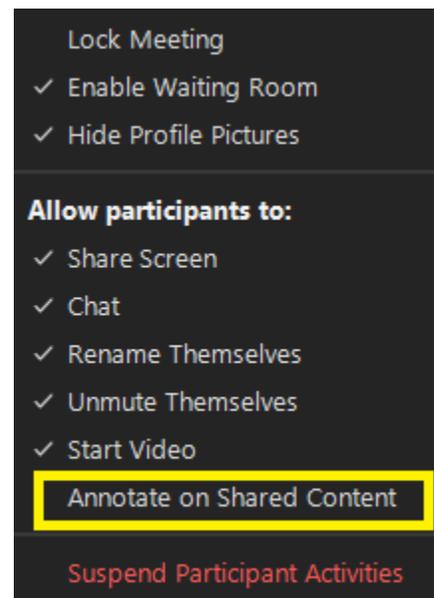
#### Who can share?

Host Only  All Participants [?](#)

#### Who can start sharing when someone else is sharing?

Host Only  All Participants [?](#)

Know that when you grant screen sharing privileges, you automatically enable the annotation function. The [annotation function](#) allows another user to “write/type” on a shared screen. As soon as you screen share, click the “Security” shield button and ensure the “Annotate on Shared Content” is disabled!



## MULTIPLE CO-HOSTS

[Use a Co-Host](#) or an [Alternative Host](#) to help monitor activity during your meeting. [Co-host and/or Alternative Hosts should have responsibilities](#) as the meeting/event begins. Some of those responsibilities may include:

1. [Disable video](#)
2. Monitor the chat

3. Check for disruptive images/video /virtual background

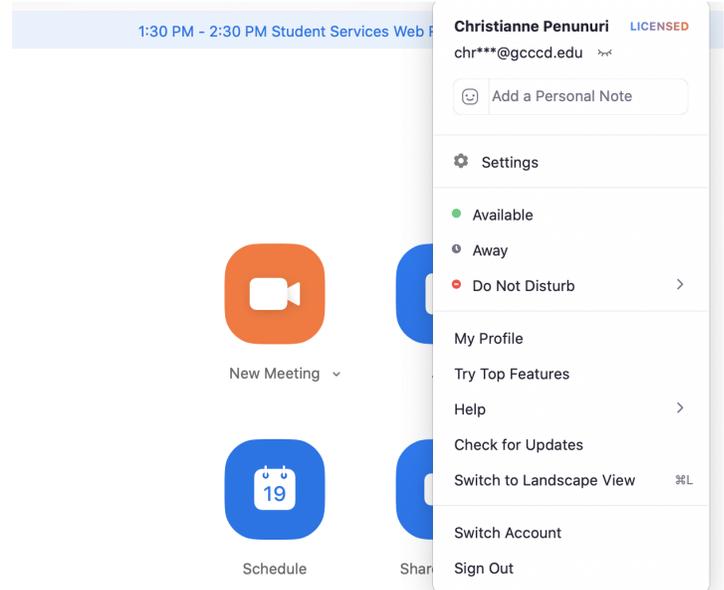
## PREPARING YOURSELF FOR ZOOM MEETINGS/EVENTS

### CHECK FOR UPDATES

Ensure your settings are updated. Zoom deploys patches and augments functionality to best meet the needs of users based upon their feedback. In your desktop profile, click in the upper right corner, and select “Check for updates.”

### ADD YOUR NAME TO YOUR PHONE

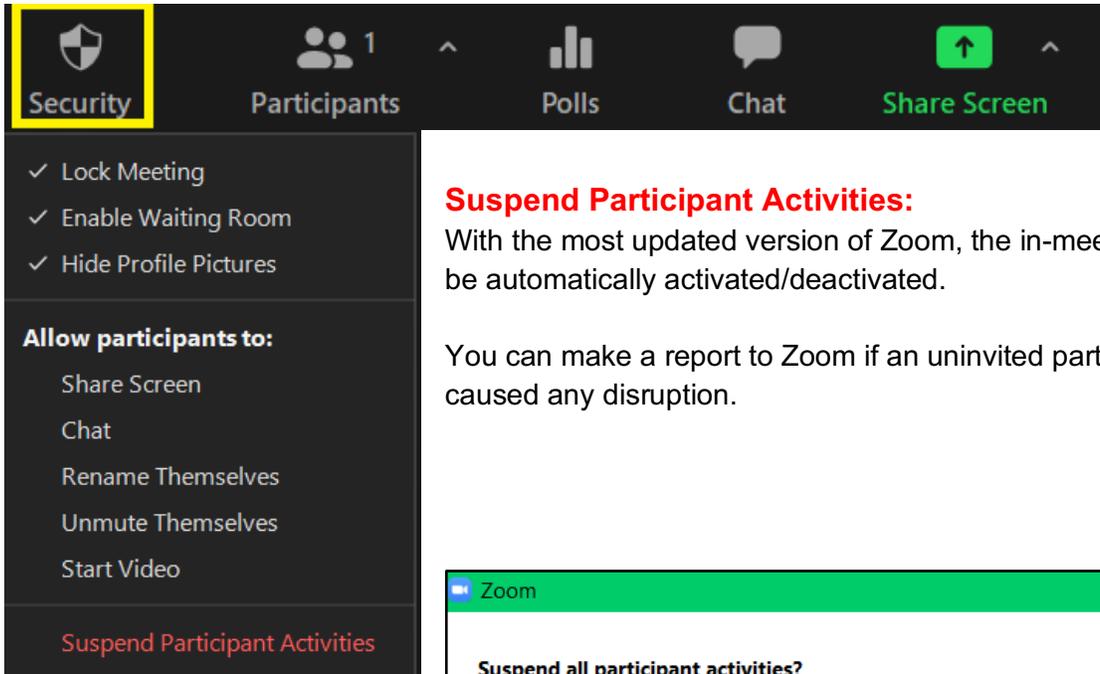
If you need to call into a meeting/event from your phone, make sure your name is listed and not just your phone number.



# IN CASE OF EMERGENCY

Should you need to remove someone from your meeting. Follow these steps:

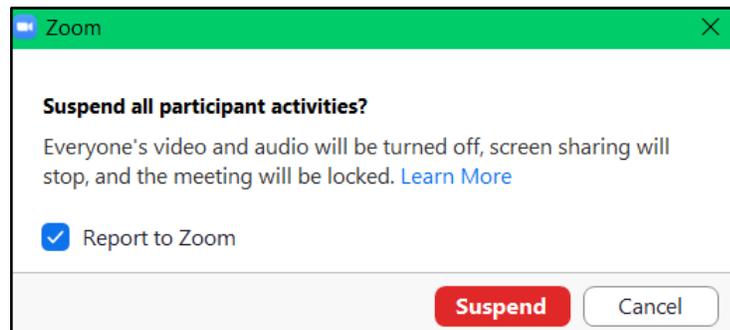
- Click the “Security” shield to ensure that your in-meeting securities are set for your meeting’s purpose. These in-meeting features can be activated/deactivated at any time during the meeting.
- [In-meeting security options](#) (below)



## Suspend Participant Activities:

With the most updated version of Zoom, the in-meeting features will be automatically activated/deactivated.

You can make a report to Zoom if an uninvited participant(s) has caused any disruption.



## Report

### Who do you want to report?

Reported users will be removed from your meeting

 ▼

### What happened?

 ▼

Include desktop screenshot [View Screenshot](#)

By sending this report, you authorize Zoom to access all data in this report, subject to Zoom's [Privacy Statement](#). This data includes screenshots, your user information, the user information of those you report, and all relevant meeting information.

**Submit**

Don't Report