

Zoom Security Best Practices & Recommendations

Do's and Don'ts at a Glance

Scheduling: The Do's	Hosting: The Do's
<ul style="list-style-type: none">• DO keep meeting passwords on• DO use automatically-generated meeting IDs• DO keep meeting links private for private meetings• DO control who you distribute classroom meeting links to• DO verify your Google Calendar sharing settings• DO set your meeting to mute people on entry• DO enable registration for a public meeting or event• DO enable the waiting room for a public event or a large class	<ul style="list-style-type: none">• DO use your waiting room to welcome attendees if you have enabled it• DO disable annotation in your meeting• DO consider locking your meeting or class after everyone has joined• DO become familiar with the security options on the toolbar• DO use the “On hold” and “Remove” features when necessary
General Security: The Don'ts	Hosting: The Don'ts
<ul style="list-style-type: none">• DO NOT share meeting URLs with anyone who is not a part of the meeting• DO NOT share meeting URLs on social media• DO NOT post meeting URLs on public calendars	<ul style="list-style-type: none">• DON'T use your Zoom Personal Meeting ID (PMI)• DON'T host alone if you're running a large meeting or class• DON'T enable Screen Sharing unless necessary

Keep Zoom Up-to-Date

- **Windows:** Open the zoom app > sign in > click your initials in the top-right corner > click "Check for Updates"
 - **macOS:** Open the zoom app > click the zoom.us menu > click "Check for Updates..."
-

Security Recommendations

General Security:

- **DO NOT** share meeting URLs with anyone who is not a part of the meeting
 - DO NOT share meeting URLs on social media
 - DO NOT post meeting URLs on public calendars
- **Keep meeting passwords on** and set a simple password
- **Add waiting room** so you can review what participants are trying to join
- Once all attendees have joined, **lock your session** ([How-To Guide here](#))
- Use "Only authenticated users can join" setting for meetings attended by people only from MLML/SJSU
- For more information, visit SJSU's [Securing Zoom Meetings page](#).

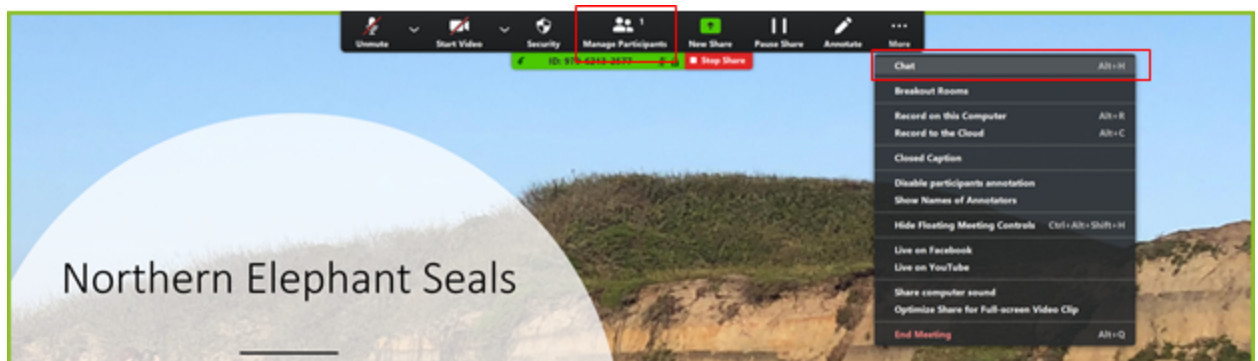
Account Security Settings:

- Sign-in to Zoom > Settings (left-side menu panel)
 - Enable Personal Meeting ID - **OFF**
 - Require a password when scheduling new meetings - **ON**
 - Require a password for instant messages - **ON**
 - Embed password in invite link for one-click join - **OFF**
 - Require password for participants joining by phone - **ON**
 - Mute participants upon entry - **ON**
 - Screen sharing- **ON**
 - Who can share - **Host Only**
-

Best Practices & Tips

- Select "**Participants**" at bottom of Zoom browser to view & manage participants
- Select "**Chat**" at bottom of Zoom browser to open chat window
- Click a participants name in the Chat window or the 3 dots in the video/profile pic to chat with them
- Tips for Hosts & Co-Hosts: Keep Participants & Chat windows open during entire meeting
- Set your name in your Zoom portal and/or app
- Let your class know that the meeting is being recorded
- Plug your phone into power when using it to record video on Camtasia or Zoom

- When you share your screen, you can select to just share a web browser or app instead of your entire desktop
 - You can select Whiteboard under Share Screen to illustrate points
- **Hide non-video participants**
 - Hover over participants thumbnail at top of Zoom Browser
 - Select the three dots
 - Select “Hide non-video participants”
- If using a conference phone for audio, be sure to mute the other computers/TVs in room that are in the meeting
- **Large Meeting Tips:**
 - Wait to admit participants until the meeting starts
 - Participants with raised hands will rise to the top of the recipient list
 - Assign multiple Co-Hosts to help moderate a large meeting
 - Pause the recording until all participants are in the meeting and the meeting starts
- **When sharing your screen, you can view the Participants and Chat windows** by scrolling to the top of your Zoom app and clicking the Participants on the Options Bar or the Chat button in the More section:



Revision #27

Created 14 May 2020 20:28:10

Updated 5 July 2023 19:17:16