Best Practices for Securing Public Zoom Meetings

As more people host their virtual events using Zoom, we wanted to offer up tips to ensure everyone joining an event does so with good intentions. Like most other public forums, it's possible to have a person (who may or may not be invited) disrupt an event that's meant to bring people together (sometimes called Zoom bombing).

Please be aware that when you schedule a meeting at Bard, waiting rooms and passcodes are **enabled by default** in the Bard Zoom domain. The Join URL that you send to your intended participants will include an encrypted version of this password, so you don't need to worry about sending the password separately.

NOTE: These tips are generally considered for public meetings, not regular classes. That said, it's good to know what options you have as a Host during any kind of Zoom meeting.

To IMMEDIATELY Suspend a Participant's Activities:

If your class or public event is getting disrupted, hosts and co-hosts can pause the meeting to remove and report the offending party and prevent further disruption. Click the **Security icon** and select **Suspend Participant Activities** to temporarily halt all video, audio, in-meeting chat, annotation, screen sharing, and recording, and end Breakout Rooms. You can resume the class by re-enabling the individual features.

To remove an offending party in your Zoom meeting:

1. Click on **Manage Participants** in the toolbar
2. Go to the panel on the right and mouse over **the participant name** you need to remove
3. Click on the **More... fly-out menu** that appears and select **Remove**.

Additional security that can be enabled to try to prevent Zoom-bombing:

- **Watch where you post Zoom links**. When you share your meeting link on social media or other public forums, that makes your event … extremely public. ANYONE with the link can join your meeting. Therefore, try not to post Zoom meeting links on public-facing websites or on social media sites. Hackers can simply search for zoom.us links on websites and find unsecured meetings to join. **Avoid using your Personal Meeting ID (PMI) to host public events**. Your PMI is basically one continuous meeting and you don't want strangers crashing your personal virtual space after the party's over. **Learn about meeting IDs** and how to generate a random meeting ID.

- **Utilize the Waiting Room**. Familiarize yourself with Zoom's settings and features so you understand how to protect your virtual space when you need to. For example, the **Waiting Room** is an unbelievably helpful feature for hosts to control who comes and goes. If you don't recognize a name that shows up in your waiting room, you don't have to give them access to the meeting room.

- **Enable a co-host** for your public meetings so that another person has host access to help you remove a disruptive guest.

- **Don't give up control of the shared screen**. You do not want random people 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, on the host toolbar click the arrow next to Share Screen and then **Advanced Sharing Options..**

- **Lock the meeting.** It's always smart to lock your front door, even when you're inside the house. When you lock a Zoom Meeting that's already started, no new participants can join, even if they have the meeting ID and password (if you have required one). In the meeting, click **Participants** at the bottom of your Zoom window. In the **Participants pop-up**, click the button that says **Lock Meeting**.

- **Set up your own two-factor authentication.** Two-factor authentication (2FA) is a two-step sign-in process that requires a one-time code from a mobile app or text message, in addition to the main Zoom sign-in. This provides an additional layer of security since users will need access to their phone to sign in to the Zoom web portal, desktop client, mobile app, or Zoom Room.

- **Disable video.** Hosts can turn someone's video off. This will allow hosts to block the video presence of unwanted, distracting, or inappropriate guests.

- **Mute participants.** Hosts can mute/unmute 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 keep the clamor at bay in large meetings.

Quickly find your in-meeting Security Settings (Hosts):

https://support.zoom.us/hc/en-us/articles/360041848151-In-meeting-security-options

Securing your virtual classroom:

https://blog.zoom.us/best-practices-for-securing-your-virtual-classroom/

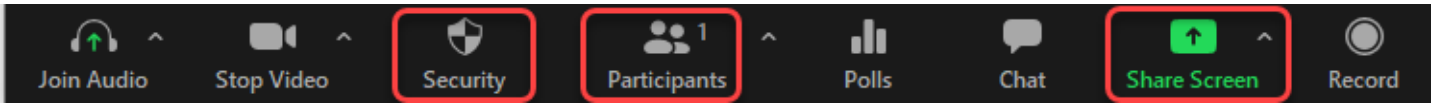
Bard Documentation on Zoom:

Bard IT Training Documentation

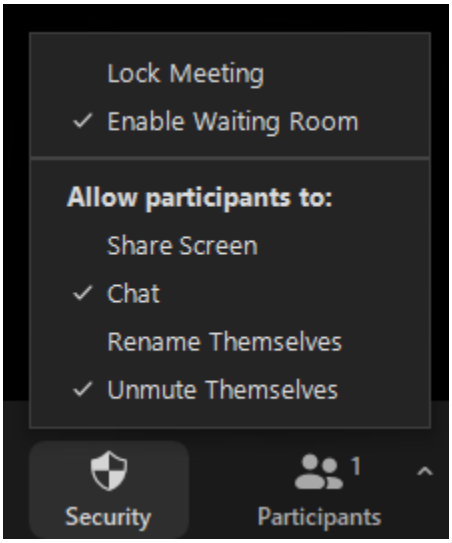
Please Check out Classes in Using Zoom at Bard:

Bard IT Training and Workshops

Important Buttons on the Host Toolbar:



Security Button Options:



Advanced Share Screen Options: