Quick Tips for Securing your Zoom Virtual Events

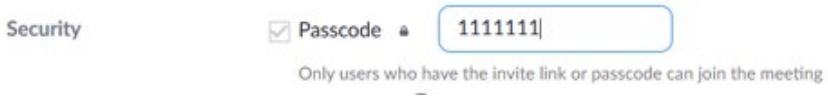
Zoom bombing is when unwanted attendee(s) enter a Zoom meeting and post disruptive video, text, and take over the meeting's screen share. To reduce the chances of Zoom bombing occurring in your Zoom meeting, we recommend the following:

- Review and follow the best practices listed below. Reach out to support@villanova.edu if you have any questions about the recommendations listed below.
- Depending on the format, goals, and size for your virtual event, consider using Zoom webinar. Reach out to support@villanova.edu and request more information on Zoom webinar.

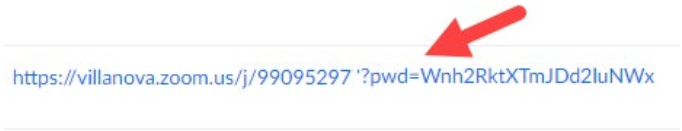
Steps to follow before your Zoom virtual event:

Require a Passcode to Join the Zoom meeting

- When scheduling the Zoom meeting, enable the "Passcode" setting. This will help secure your meeting because if a Zoom bomber is randomly trying different meeting IDs, they will not able to enter the meeting because they do not have the passcode (as long as you do not share the passcode on public-facing sites). The attendees should not need to know the specific passcode because the meeting weblink URL will contain the password within the URL weblink itself (see picture below)



Meeting URL Weblink with Passcode included:



Do not post Zoom link on public-facing sites (websites, social media)

- This opens the door for anyone (including unwanted guests) to join your meeting. To share the Zoom link with your participants, we strongly recommend that you utilize some sort of registration system, where interested attendees fill out a form with their information, and then the Zoom link is provided after that form is completed. This will allow you to post a link to the registration on public-facing sites, rather than the link to the meeting itself.

Please check with your department/College about specific registration tools that they currently use. Zoom meeting has a registration feature as well. Information on how to use the Zoom Registration is available here.

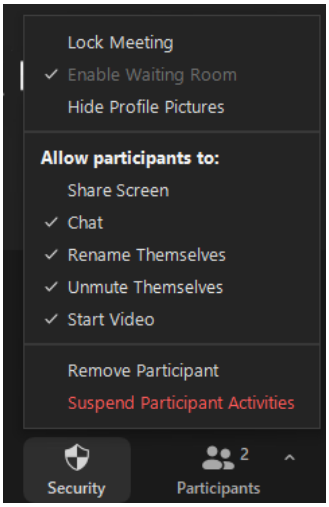
Utilize Alternative/Co-host to help admit users

- By default, all Villanova Zoom meetings have a waiting room enabled. You should have a co-host to help admit attendees into the meeting. This will give you more time to review user(s) in the waiting room. Instructions on how to set up an alternative host or co-host.

Steps to follow during your meeting:

Security Tool

- Zoom now puts all your essential security options in a single button called "Security" right in the in-meeting menu. Familiarize yourself with these settings, especially "Suspend Participants Activities" and "Remove Participant".



Lock meeting (Prevents people from entering the meeting)

Share Screen (Allows you to control if participants can share screen. *Recommendation: Turn off unless it is specifically required*)

Chat (allows you to disable the chat for everyone, except the host/co-host)

Rename Themselves (Allows you to control if participants can rename themselves)

Unmute Themselves (Allows participants to unmute themselves without the host's permission)

Start Video (Allows participants to share their video without the host's permission.)

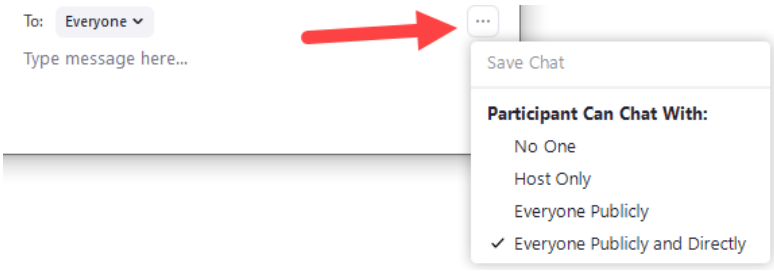
Suspend Participants Activities (With one-click, turn off all participant's video, audio, ability to share their screen, and lock the meeting.

Remove Participant (Removes of a participant from a meeting. Participant can not re-join unless "Allow removed participants to rejoin" is enabled in Meeting settings)

Configure your Chat settings

- Since Zoom bombing can happen in the chat area, the host should edit the chat option and change it to "Host Only" (open Chat and click on the ellipsis symbol "…"). By selecting "Host Only", participant messages go only to the host and co-hosts. Only the Host/Co-Host can send messages to everyone. You can also select "No One", which disables in-meeting chat (hosts/co-hosts can still send messages to everyone).

  If you plan to utilize chat for interaction during the virtual event, you should enable chat during the period of interaction and then change it to one of the more secure settings listed above outside of that period of interaction.



Consider disabling the "Participants Renaming Themselves" setting.

- While the Participants Renaming Themselves is helpful to allow participants to correct how their name displays within Zoom, it can allow Zoom bombers to rename themselves with a name to blend in with the rest of the event. Once the virtual event has started (which allows legitimate participants to rename themselves if needed), please consider disabling the "Participants Renaming Themselves" setting.