**Best Practices in Zoom to prevent Zoombombing:**

We have learned that even with some of the simple best practices in zoom it is easy for trolls to enter and disrupt zoom meetings. Here are some best practices that you can use to reduce the chances of getting bombed.

1. When setting up a meeting select generated ID instead of personal ID so the meeting as a unique ID.
2. Require a meeting password.
	1. If someone uses the meeting link, they will not need the password.
	2. If they use the meeting ID, they will be prompted for the password.
	3. If you are posting the link in a public place you will want to either have a link that will prompt an email to one person to vet out and send a link to or just send the meeting ID and have them contact you for the password.
3. Click on Advanced Options and enable waiting room.
	1. You’ll want to have a host monitor the participants panel for people in the waiting room. That host will vet out and allow people into the meeting.
	2. This will not only help make sure only people there for the meeting are in the actual meeting, but it will prevent people from joining during the meeting.

There are some other best practices to keep in mind:

1. Make sure the Enable join before host is unchecked.
2. Add in the alternative hosts in the meeting invite or have the hosts select a co host when everyone gets in the meeting.
3. If you do end up getting bombed the host should end the meeting for all participants as soon as possible and send a new link with new password out to participants. People are coming in large groups making it impossible to keep up with removing them from the meeting.