HCC Security Advisory

04/02/2020

"Zoom-Bombing" Affects Meetings and Classrooms Nationwide

As large numbers of schools turn to video-teleconferencing (VTC) platforms to stay connected and continue instruction in the wake of the COVID-19 crisis, reports of VTC hijacking (also called "Zoom-bombing") are emerging nationwide. The FBI and other law enforcement agencies have received multiple reports of conferences being disrupted by pornographic and/or hate images and threatening language.

"Zoom-bombing" occurs when an unauthorized person or a valid participant enters a Zoom meeting and exploits built in features of the tool to take over presenting, share unapproved content, or obtain restricted information. The best way to prevent "Zoom-bombing" is to correctly set up meeting options:

1. Use a Unique ID for Large or Public Meetings

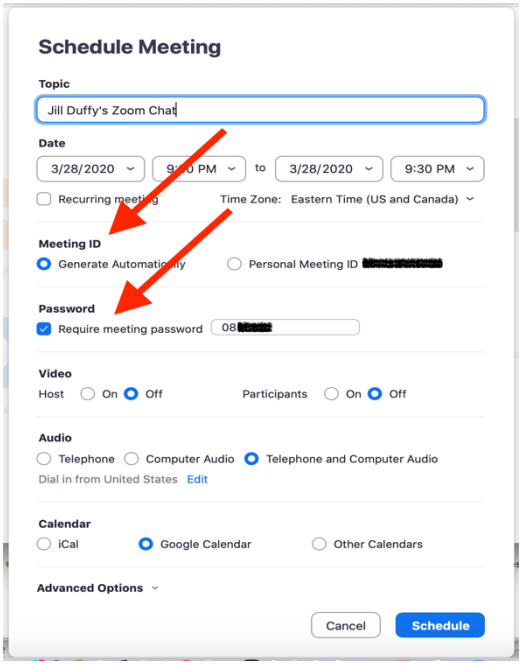
When you create or are assigned a Zoom account, the app assigns you a Personal Meeting ID (PMI). It's a numeric code that you can give out to people when you want to meet with them. You can use it over and over; it doesn't expire.

- Use this Personal Meeting ID (PMI) for standing meetings, such as weekly staff meetings or progress checks.

Zoom also gives you the option to not use your PMI for a meeting and instead generate a unique code.

- If you're the host of a large Zoom call where members of the public or other strangers are invited, it's much better to use a one-time code rather than your PMI.

When you schedule a Zoom meeting, look for the "Meeting ID" options and choose "Generate Automatically". Doing so plugs up one of the biggest holes that Zoom-bombers can exploit.



2. Require a Meeting Password

To password-protect a meeting, start by scheduling a meeting and checking the box next to Require meeting password. It's only an option when you generate a unique ID, not when you use your PMI. You'll see a numeric password, which will work for everyone who has it.

3. Create a Waiting Room

The Waiting Room feature is one of the best ways to protect your Zoom virtual classroom and keep out those who aren't supposed to be there. When enabled, you have two options for who hits the Waiting Room before entering a class:

- "All Participants" will send everyone to the virtual waiting area, where you can admit them individually or all at once. If you see names you don't recognize in the Waiting Room, you don't have to let them in at all.
- "Guest Participants Only" allows known students to skip the Waiting Room and join but sends anyone not signed in/part of your school into the virtual waiting area.

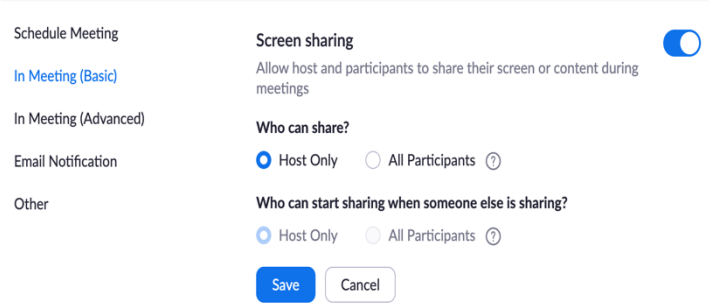
The virtual Waiting Room can be enabled for every class (in your settings) or for individual classes at the scheduling level. *Update: Starting March 31, 2020, the Waiting Room feature will be automatically turned on by default.*

4. Lock Your Virtual Classroom

Did you know you can lock a Zoom session that's already started, so that no one else can join? It's kind of like closing the classroom door after the bell. Give students a few minutes to file in and then click "Participants" at the bottom of your Zoom window. In the "Participants" pop-up, click the button that says "Lock Meeting".

5. Control Screen Sharing

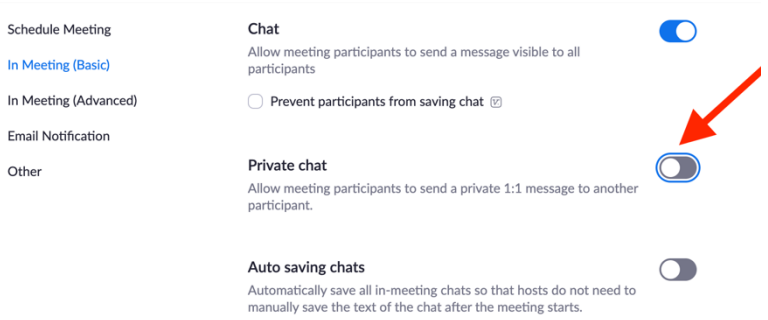
To give instructors more control over what students are seeing and prevent them from sharing random content, Zoom for education users has "Sharing privileges" now set to "Host Only," so teachers by default are the only ones who can share content in class.



- If students need to share their work with the group, you can allow screen sharing in the host controls.

6. Lock Down the Chat

Teachers can restrict the in-class chat so students cannot privately message other students. We'd recommend controlling chat access in your In-meeting Toolbar controls (rather than disabling it altogether) so students can still interact with the teacher as needed.



7. Remove a Participant

If someone who's not meant to be there somehow manages to join your virtual classroom, you can easily remove them from the Participants menu. Hover over their name, and the "Remove" option (among other options) will appear. Click to remove them from your virtual classroom, and they won't be allowed back in.

8. Additional Options for Successful Zoom Meetings

a. Disable Participant Cameras

Hosts can turn off any participant's camera. If someone is being rude or inappropriate on video, or their video has some technical problem, the host can open the “Participants” panel and click on the video camera icon next to the person's name to turn it off.

b. Mute Upon Entry

You can also mute everyone automatically when they join a call. Before the call starts, go to the web portal and navigate to “Settings” > “Meetings” and choose the meeting. At the bottom of the screen, click to “Edit” the meeting. Look for “Meeting Options” and check the box next to “Mute Participants Upon Entry”.

c. Require Registration When Setting Up The Meeting

This option shows you every email address of everyone who signed up to join your class and can help you evaluate who’s attending.

d. Allow Only Authenticated Users to Join

Checking this box means only members of your school who are signed into their Zoom account can access this particular class.

e. Disable Join Before Host

Students cannot join class before the teacher joins and will see a pop-up that says, “The meeting is waiting for the host to join.“

f. Manage Annotation

Teachers should disable participant annotation in the screen sharing controls to prevent students from annotating on a shared screen and disrupting class.