Beware of 'Zoom Bombing'

As people, businesses and education have become increasingly reliant on video chatting since the coronavirus pandemic began, the FBI's Boston office reported this week that "zoom bombing" incidents are occurring across America. A disruption specific to the teleconferencing app Zoom, which has recently surged in popularity, this vulnerability has been exploited by hackers, with disturbing results.

We are sharing a set of practices to help ensure that your meetings are free of disruption as we continue forward with Zoom.

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.

Control screen sharing

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

However, if students need to share their work with the group, you can allow screen sharing in the host controls. Click the arrow next to Share Screen and then Advanced Sharing Options. Under "Who can share?" choose "Only Host" and close the window. You can also change the default sharing option to All Participants in your Zoom settings.

Enable the 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:

1. All Participants will send everyone to the virtual waiting area, where you can admit them individually or all at once.
2. 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.

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.

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.

Security options when scheduling a class

The cool thing about Zoom is that you have these and other protection options at your fingertips when scheduling a class and before you ever have to change anything in front of your students. Here are a few of the most applicable:

- Require registration: This shows you every email address of everyone who signed up to join your class and can help you evaluate who's attending.
- Use a random meeting ID: It's best practice to generate a random meeting ID for your class, so it can't be shared multiple times. This is the better alternative to using your Personal Meeting ID, which is not advised because it's basically an ongoing meeting that's always running.
- Password-protect the classroom: Create a password and share with your students via school email so only those intended to join can access a virtual classroom.
- 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.
- 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."
- Manage annotation: Teachers should disable participant annotation in the screen sharing controls to prevent students from annotating on a shared screen and disrupting class.

Manage Participants:

The meeting host has a variety of controls they can use to secure their meeting.
For more information, visit https://support. zoom.us/hc/en-us/articles/115005759423

- **Attendee On-Hold:** if you need a private moment, you can put attendees on-hold. The attendee's video and audio connections will be disabled momentarily. Click on the attendee's video thumbnail and select Start Attendee On-Hold to activate this feature.
- Disabling Video: Instructors can turn participant video off and request to start participant video. This will allow instructors to block unwanted, distracting or inappropriate gestures on video.
- **Mute participants or Mute All:** Instructors can turn mute / unmute participants or all. This will allow instructors to block unwanted, distracting or inappropriate noise from the meeting. You can also enable "Mute Upon Entry" and uncheck "Allow participants to unmute themselves"
- **Turn off file transfer:** In-meeting file transfer allows people to share files through the in-meeting chat. Toggle this off to keep the chat from getting bombarded with unsolicited pics, GIFs, memes, and other content.

- **Turn off annotation:** You and your attendees can doodle and mark up content together using annotations during screen share. You can disable the annotation feature in your Zoom settings to prevent people from writing all over the screens.

Manage Recordings:

You can further secure recordings by password-protecting them or restricting download access. You can also manage your recording settings to only record the "Active speaker and shared screen" excluding the gallery view. You can also uncheck "Display participants names" and in the recording.

Email Tips:

Because of all the cyber-attacks against Zoom technology it is highly encourage to not click any links for a Zoom meeting you receive by Email. If you're not sure don't click it. An option to sending Email would be to create a page inside Canvas with a link for your Zoom meeting, or post it in a class announcement.