WAKE FOREST UNIVERSITY

Remote Teaching Updates & Resources

1 message

Betsy Barre <barreea@wfu.edu> Sun, Mar 29, 2020 at 7:00 AM
Reply-To: Betsy Barre <barreea@wfu.edu>
To:

Troll-Proofing Your Zoom Sessions

By Hannah Inzko on Mar 28, 2020 08:40 pm

Much like those students who have stumbled into your classroom by mistake, it's possible to have a person (who may or may not be invited) disrupt a class and make it difficult to continue teaching.

So, how do we ensure our students make it to the right class? How do we keep out any unwanted or uninvited guests? What do we do if someone shows up in our Zoom classroom with nefarious motives? What is, and how do you avoid, Zoom-bombing?

The term Zoom-bombing refers to those uninvited guests that wander into your Zoom classroom and use the screen-sharing feature to interrupt your class and distract your students.

It should be said that most Zoom-bombing happens when meeting links are posted publicly, for example, if you are trying to post "office hours" for a broader community than just one class, but depending on your personal settings, some

seemingly private meetings may also be vulnerable. Below are a few remote-classroom strategies that ensure your meetings (both public and private) are not disrupted.

Securing entrance to your class

Create a waiting room for your students, and you can even personalize the message they see when they follow your link, so they know they're in the right spot. This message is really a great spot to post the class name, your name and any rules/guidelines for your class.

Even for Zoom sessions created within the LMS, there is an added layer of security when you require a password for students before entering your room. They will still need to wait in the "Waiting Room" if you have one set-up, but at least you will know that they had the appropriate credentials for the class.

Once all of your students have made it into your class, you are able to lock your meeting so that no one else can wander in, accidentally. Just note that this would block entry to any students trying to join late, or rejoin if they get disconnected.

Keeping disruptions out

Most Zoom-bombing events can be handled by adding security to your classroom entrance, so the options below may be more than you need. But if you were thinking of opening up Zoom sessions to folx outside of your class or Wake Forest community, they may prove helpful.

It should also be said that there are really good reasons to allow, and even encourage, students to share their screen, share files, use the chat feature, and annotate during screen share. But these setting options are available to hosts as a layer of security.

- Disable video: Hosts can turn someone's video off. This will allow hosts to block distracting, or accidental video snafus, because we all know these happen.

- 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.
- 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 distracting 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.
- Disable private chat: Zoom has in-meeting chat for everyone or participants can message each other privately. Restrict participants' ability to chat amongst one another while your event is going on and cut back on distractions or getting unwanted messages during class.

Taking back control

If you have secured your Zoom sessions and you still find yourself with a disruptive or distracting participant, there are ways to remove them from class. My advice would be to set expectations for behavior at the start of class so that removal doesn't come as a surprise.

- Remove unwanted or disruptive participants: From that Participants menu, you can mouse over a participant's name, and several options will appear, including Remove. Click that to kick someone out of the meeting.
- Allow removed participants to rejoin: When you do remove someone, they can't rejoin the meeting. But you can toggle your settings to allow removed participants to rejoin, in case you boot the wrong person.
- Put 'em on hold: You can put everyone else on hold, and the attendees' video and audio connections will be disabled momentarily. Click on someone's video thumbnail and select Start Attendee On Hold to activate this feature. Click Take Off Hold in the Participants list when you're ready to have them back.

The upside is that you only have to go through and choose your preferred security settings once, and they will persist throughout all future meetings. Now, let's go connect with our students!

Subscribe

Receive CAT remote teaching updates in your inbox.

WFU Email Address

Subscribe

The post Troll-Proofing Your Zoom Sessions appeared first on Center for the Advancement of Teaching.

Read in browser »

Recent Articles:

Remote Podcasting
Failure, Resilience, and a Virtual Happy Hour!
Communicating with Canvas: A Few Simple Tools
Let's Talk about Grades
Going Remote: Planning, Challenges, and More