EDUCATION WEEK

How to Thwart 'Zoombombing' in the Remote Classroom: 10 Tips

By **Alyson Klein**

September 22, 2020

Back to Story

New Hampshire's Concord High School was hit with a quadruple whammy on the second day of online-only school: Racial slurs were posted on the chat in one virtual classroom. Two others were exposed to pornographic images. And another group of students saw a picture of a fake gun appear during a videoconferencing lesson.

In all four cases, teachers quickly kicked the intruders out of the Zoom conferencing platform. But the incidents were a big headache for teachers, administrators, and perhaps especially, kids.

"Many of the students were like, 'We don't want to have this getting ruined,'" said Kaileen Chilauskas, the school's assistant principal, who spoke to the impacted classes a few days after the intrusions. Zoom is the only way they can interact with their teachers and continue learning, kids noted.

But such interruptions, known as "Zoombombings" or "Zoom raids" even though they can happen on any video conferencing platform, are becoming an all-too common occurrence, according to dozens of published reports.

For instance, in Hindsdale, Ill., an 8th grader "mooned" two high school classrooms and yelled out a racial insult. A high school geometry class in San Antonio was interrupted by someone using the name of a student in the class, and an image of two Ku Klux Klansmen. And in Schuylkill County, Pa., someone interrupted kindergarten orientation, yelled racial slurs, cursed, and threatened children.

Media coverage probably isn't capturing the full scope of the problem, said Doug Levin, the founder and president of the K-12 Cybersecurity Resource Center. He expects that the interruptions are happening in the majority of school districts.

Students will be in an online class, all working together. Then, suddenly, someone “starts streaming porn, or all of this racially charged stuff," Levin said. "It's like a stranger walked off the street and started stripping and yelling at the kids. That's essentially what's happening online."

It's often unclear if kids in the school are behind these incidents or whether it is someone from the outside, who may have gotten passcodes from students, off of a school website, or just guesswork, educators said.

Complicating matters: Some people, presumably students, are inviting "Zoombombers" in posts on social media platforms, including Twitter and TikTok, using hashtags like #zoomraid.

"Raid this math class," one tweet read, giving a class time, meeting credentials, and encouraging would-be disrupters to "use a realistic name." Another urged, "Raid my civics class be racist." One user openly wondered if teachers would be able to tell who gave away class credentials.

What Can Educators Do?

10 Tips for Curbing ‘Zoombombing’

Classrooms around the country have been interrupted by so-called “Zoombombers” or “Zoomraiders,” who shout obscenities, share sexual images, or racist content in the middle of an online lesson. Despite the name, the incidents can take place on any video conferencing platform, not just Zoom.

Here are 10 steps educators and experts say school districts and teachers can take to curb this problem:
1.) Offer teachers professional development on how to block would-be Zoombombers. One district created two, 40-minute videos, each exploring a different online conference platform.
2.) Make sure students are required to have a password to get into virtual classrooms.
3.) Continually change the online

credentials for virtual classrooms, and don’t post them to external websites.
4.) Have a waiting room for each videoconferencing lesson. Teachers should only “let in” students who are on their roster.
5.) Don’t admit a student to a virtual classroom if someone under their name is already in class. That person could be an impostor.
6.) Teachers should show up to the online classroom first. That way, students are not there unsupervised.
7.) Ensure that only the teacher can share the screen, unless there’s a reason for students to share their screens.
8.) Disable students’ ability to transfer files back-and-forth in class.
9.) Disable chat unless you are using it for a clear reason.
10.) Make sure students understand the rules of a virtual classroom, just like they would in a brick-and-mortar one.

So what can teachers and districts leaders do about these interruptions?

Professional development is key. North Carolina's Winston-Salem/Forsyth created two, 40-minute long instructional videos for staff, one for Microsoft Teams and another for Zoom.

The videos "show teachers click-by-click the best way to set up their environment," said Kevin Sherrill, the district's assistant superintendent for technology. "We're encouraging teachers to educate themselves. We have 500 teachers, and we can't be with them every minute, so they just have to learn. It's not an easy task."

The videos embrace best practices, including ensuring the online conference room is set up so participants need a password to get in, and that there's a waiting room.

Teachers should be careful in figuring out who can come in from that waiting room, making sure the same kid isn't trying to enter the class twice. One of the entrants might not be the real student.

"I think when they are impersonating the name of an actual student that makes it much tougher for teachers," said Pam McLeod, director of tech and information security officer for the Concord school district. "Some folks were using a name of someone who might already be in class."

She also suggested that teachers continually change the credentials of their online conference, to make it harder for students to share them with would-be bombers.

Another tip: Don't post links to Zoom, Microsoft Teams, or other conferencing platforms to external websites, Sherrill said. That appeared to lead to interruptions in his district.

What's more, teachers—who are typically the "host" of the conference—should be able to show up to class first and let students through the virtual door. That way, kids can't do disruptive things in the room while they are unsupervised, waiting for class to start, suggested Amy McLaughlin, the director of the cybersecurity project at the Consortium for School Networking.

‘Take It Really Slow’

Educators might also want to hold off before trying to use many of the features of conferencing platforms to limit opportunities for the system to be compromised.

Teachers should consider "not trying to do everything that your platform offers you in the first day of class," Chilauskas said. "Teachers get enthusiastic about every platform that's out there. You've got to take it really slow before you give them these options, the chat function, polls that you can have the kids take, kids ability to mute and unmute themselves."

What's more, teachers' aides can help monitor the technical aspects of videoconferencing. "It's hard to oversee 30 spaces in a Zoom call," Chilauskas said. "Even just having that extra adult support is really helpful." She also encourages students to keep their cameras on so that the teacher can see that it is really them, and not a possible impostor.

McLaughlin noted that conferencing platforms can also control screen sharing so that only the "host" (teacher) can share. That makes it tougher for hackers, or students, to flood the screen with inappropriate images or video. The set-up can be changed if a teacher needs students to be able to share their screens for educational purposes, such as a presentation.

And she recommends disabling students' ability to transfer files back-and-forth in the classroom, which she likened to "passing notes" in class.

In the same vein, teachers should have clear expectations around the chat function in their mobile conferencing platforms and may want to disable it at times. Teachers should not allow students to "have a back-channel chat conversation because that's like whispering" in class, McLaughlin said.

'That Teachable Moment'

It is very important for students to understand the rules of a virtual classroom, just like they would a brick-and-mortar one, McLaughlin said.

Some suggestions: Require students to have their name on display, so the teacher knows who they are. Make it clear that they are not allowed to invite outside members to class. And let students know that if they behave badly, they can be asked to leave the conference room, just like they would a regular classroom. Some school districts have taken formal disciplinary–or even legal–action against students who have disrupted class.

"You can't just assume that students are all of a sudden" going to understand those things intuitively, McLaughlin said. "They've gone from in-person to online [instruction] and don't know what the rules are."

But despite educators' best efforts, Zoombombers can still sometimes get into classes. So what should educators do if that happens?

Let parents know right away, said Bernard Watson, the director of media relations for the 177,000-student Gwinnett School District outside Atlanta. The district also does not treat all incidents equally. Some are referred for disciplinary action—for instance, if a student is yelling or cursing at the teacher. But others—including those involving behavior such as displays of nudity—might be referred to local law enforcement. So far, Gwinnett has had seven such instances since the start of the school year, Watson said.

Talk to students about the incident, Chilauskas suggested. After Concord's four Zoombombing incidents in a single day, she sent an email to parents and then followed up with the classes later in the week. The students were understandably upset, Chilauskas said. One girl worried someone could enter a class under her name and disrupt it. "I did assure her that people are not as anonymous as they think," Chilauskas said.

Giving students a chance to discuss what happened is the right call, McLaughlin said. She suggested teachers tell students, "'Let's talk about why this was inappropriate. Let's talk about why this was harmful.'" she said. "To my mind, this really presents that teachable moment."

WEB ONLY