Holding Class on Zoom? Beware of These Hacks, Hijinks and Hazards

By Tony Wan   Mar 27, 2020 EdSurge

This article is part of the guide Sustaining Higher Education in the Coronavirus Crisis.

On Tuesday, Kristina Ishmael was watching a webinar about how coronavirus will impact K-12 education policy, when the screen was suddenly flooded by pictures of pornographic images and racial slurs.

The moderator turned off the video—but to no avail. The perpetrator later took control of the audio, and Ishmael, a senior policy manager of education policy at New America, recalls a male voice spewing misogynistic epithets.

What she and about 100 other participants experienced now has a name: "Zoombombing." It's essentially internet trolling on video conferencing, involving somebody who takes over the audio and video controls to broadcast inappropriate materials and remarks.

The term was virtually nonexistent until last week, when the shuttering of schools and business places across the country led many people on try video-conferencing tools. The most popular has been Zoom, which has reported a surge in new users. Among them are educators, who have taken up the company's offer to remove the 40-minute limit normally imposed on Basic accounts for all K-12 schools.

But as Zoom has grown in popularity, so have episodes of internet impropriety. Like journalists and investors, educators from New York City to the University of Southern California have reported instances where their virtual meetings were hijacked by miscreants.

New tools often come with learning curves. And as many parents, teachers and students take to virtual conferencing tools for the first time, they are zooming into a "digital Wild West" fraught with as many risks as rewards, says Eric Butash, director of education technology at Foster-Glocester Regional School District in Rhode Island.

Protect yourself and others from getting Zoombombed.

Zoombombing can take different forms, though it is not as sophisticated as it may sound. Usually, it entails an unsavory character who finds a Zoom link shared on public channels like Twitter, accesses a meeting that does not require a password, and abuses the chat, screen-sharing and file transfer privileges that the meeting organizer has not restricted.

But it has been enough of a concern that it was the subject of an email sent on March 24 by USC's president and provost to its community. The note began:

"We are sorry to report we learned today that some of our online Zoom classes were disrupted by people who used racist and vile language that interrupted lectures and learning. We are deeply saddened that our students and faculty have had to witness such despicable acts."

The email directs students and faculty to a dedicated "Zoombombing Resources" page that USC officials created on its website. The page walks through what controls conference organizers can use to secure meetings, remove participants, and disable screen-sharing and audio features that can be abused.

Zoombombing doesn't always involve internet strangers. Sometimes, students share links with their peers from other classes and schools, who can also wreak havoc.

Michelle Pacansky-Brock, a faculty mentor at California Community Colleges, has compiled a set of tips specific for instructors leading online classes. Zoom has also outlined steps to help organizers secure their meetings against unwelcome guests.

Students do not need Zoom accounts to join a virtual class.

Zoom does not require participants to have individual accounts in order to join a meeting. For students, it's best to keep it that way, advises Butash. "Students should never be making an account in Zoom," he says. "That's where it can get districts into trouble."

In addition to video conferencing, Zoom also has live chat features that allow anyone with an account to message each other directly. In a typical school setting, such digital communications would be subject to monitoring or outright restricted.

For schools and districts that have signed up for Zoom, Butash says "it is a must" to use a single sign-on provisioning tool so that school technology administrators can control permissions and privileges for staff accounts, and disable features that are unnecessary or inappropriate. His district used Clever, which recently enabled a Zoom integration for its K-12 customers. (The company says more than 2,000 school districts that use its provisioning services have also done this.)

When teachers schedule a Zoom meeting, all they need to do is to share the URL with students, who do not need their own Zoom accounts to join. That link should be shared through a learning management system, an existing school-managed communication tool, a private class webpage or another secure portal (but never publicly).

In Butash's district, school officials have disabled the camera and muted the microphone for students upon joining a Zoom conference. They also cannot enter a room unless the teacher is already present, so that students cannot chat among themselves unsupervised.

Should you record lessons?

Teachers have also recorded their lessons on Zoom and other video-conferencing tools, so that they can be made available later to students who were not able to attend the session. But Butash discourages educators in his district from doing so, especially if children are captured in the video.

Any images or recordings that include students' faces or names make these materials an "education record" according to FERPA, which has strict rules around how photos and videos can be accessed, stored and shared.

If a lesson must be recorded, teachers should record only parts where they are speaking, and refrain from capturing any audio or video of students before the class or during follow-up discussions, suggests Amelia Vance, the director of youth and education privacy at the Future of Privacy Forum.

Zoom can still serve as a handy, private virtual space for recording lessons, provided no students are present, says Butash. "We do encourage teachers to go into Zoom themselves, and record themselves giving a presentation without any kids in the room" that can be distributed later.

Do not post screenshots of your class online!

"As a communications platform, the privacy of Zoom depends in part on the practices of its users," says Emily Tabatabai, a partner specializing in privacy at the law firm Orrick, in an email. "The very nature of a video communications platform presents some risks of data leakage that could potentially violate the school's obligations under FERPA or other student privacy laws."

Already, some enthusiastic teachers and parents eager to show off their Zoom classes online have unwittingly violated student privacy rules. On social media, they have posted tiled, Brady-Bunch style screenshots of their classes on Zoom and other web conferencing tools.

Butash says he can understand their eagerness to share the excitement of holding a class online for the first time. But there's one major problem: Many of these pictures often include not only students' faces—but their full names.

Sharing these screen captures online "is a horrible idea that violates a lot of social media policies," says Vance. Unless in very specific—and rare—cases where a school and parent has signed off on media agreements authorizing the use of students' name and image, posting such photos online is a violation of FERPA and COPPA rules.

This blunder is not unique to video-conferencing tools; educators have posted identifiable pictures images of students on social media in the past. But the emergence of Zoom has resurfaced this problem.

Simply put, "teachers, you can get in trouble for this," says Vance.

What about Zoom's school privacy policies?

A standard Zoom account is "not at all" compliant with FERPA, COPPA or state student privacy laws, according to Vance, and should not be used by schools or students in any official educational capacity. Recent analyses from Consumer Reports and Motherboard have found that the app shares data with third parties including Facebook.

Zoom also offers paid subscriptions specifically for use in schools and colleges. On its website, the company maintains it is committed to "ensuring that our customers in the education sector are compliant with the Federal Education Rights and Privacy Act."

The company recently added a privacy policy specific for K-12 schools and districts, which it says is "designed to reflect our compliance" with student privacy laws. A Zoom spokesperson said in an email that for teachers and school officials who have signed up for the free, upgraded basic Zoom account, "their basic license is still compliant with FERPA and COPPA."

However, whether Zoom's K-12 school privacy policy and practices remain in effect when students and teachers use it at home for online classes or other instructional affairs remains an open question.

"Parents should also understand that Zoom's student privacy practices and restricted data use policies may apply only when the service is used by K-12 schools for an educational purpose," says Tabatabai, of Orrick. "Parents should exercise oversight in monitoring how their children may be using Zoom through a personal account outside the school environment."

Tony Wan (@tonywan) is Managing Editor at EdSurge, where he covers business and financing trends in the edtech industry. Reach him at tony [at] edsurge [dot] com.