Security tips every teacher and professor needs to know about Zoom, right now

reader comments

55 with 42 posters participating

Share this story

With the Coronavirus pandemic forcing millions of people to work, learn, and socialize from home, Zoom conferences are becoming a default method to connect. And with popularity comes abuse. Enter Zoom bombing, the phenomenon of trolls intruding into other people's meetings for the sole purpose of harassing attendees, usually by bombarding them with racist or sexually explicit images or statements. A small sample of the events over the past few days:

- An attendee who disrupted an Alcohol Anonymous meeting by shouting misogynistic and anti-Semitic slurs, along with the statement "Alcohol is soooo good," according to Business Insider. Meeting organizers eventually muted and removed the intruder but only after more than half of the participants had left.
- A Zoom conference hosting students from the Orange County Public Schools system in Florida that was disrupted after an uninvited participant exposed himself to the class.
- An online meeting of black students at the University of Texas that was cut short when it was interrupted by visitors using racial slurs

The basics

As disruptive and offensive as it is, Zoom bombing is a useful reminder of just how fragile privacy can be in the world of online conferencing. Whereas usual meetings among faculty members, boards of directors, and employees are protected by physical barriers such as walls and closed doors, Zoom conferences can only be secured using other means that many users are unversed in using. What follows are tips for avoiding the most common Zoom conference pitfalls.

Make sure meetings are password protected. The best way to ensure meetings can be accessed only when someone has the password is to ensure that Require a password for instant meetings is turned on in the user settings. Even when the setting is turned off, there's the ability to require a password when scheduling a meeting. It may not be practical to password protect every meeting, but conference organizers should use this measure as often as possible.

When possible, don't announce meetings on social media or other public outlets. Instead, send messages only to the participants, using email or group settings in Signal WhatsApp or other messenger programs. This advice is especially important if you're the leader of a country, such as the UK. (Fortunately, Prime Minister Boris Johnson had password protected the meeting and was prudent enough not to have included the passphrase in his tweet. Even then, his tweet divulged the IDs of multiple participants.)

Carefully inspect the list of participants periodically, whenever possible. This can be done by the organizer or trusted participants. Any users who are unauthorized can be booted. (More about how to do that later.)

Carefully control screen sharing. The user settings allow organizers to set default sharing settings by default. People who rarely need sharing should turn it off altogether by

sliding the button to the right to off. In the event participants require screen sharing, the slider should be turned on and the setting for only the host to share should be turned on. Organizers should allow all participants to share screens only when the host knows and fully trusts everyone in a meeting.

And while you're at it

The four measures above are cardinal. Here are a few other suggestions for securing Zoom meetings:

Disable the Join Before Host setting so that organizers can control the meeting from its very start.

Use the Waiting Room option to admit participants. This will prevent admittance of trolls should they have slipped through the two cardinal defenses.

Lock a meeting, when possible, once it's underway. This will prevent unauthorized people from joining later. Locking a meeting can be accomplished by clicking Manage Participants and using the controls that appear on the right of the meeting window. Manage Participants also allows an organizer to mute all participants, eject select participants, or stop select participants from appearing by video.

Be aware of everything that's within view of your camera. Whether working from home or an office, there may be diagrams, drawings, notes, or other things you don't want other participants to see. Remove these from view of the camera before the meeting starts.

Beyond the above advice, Zoom users should consider using a browser to connect to meetings rather than the dedicated Zoom app. I prefer this setting because I believe the attack surface on my system—that is, the number of vulnerabilities a hacker can exploit to breach my security—grows with each app I

install. In 2020, most browsers are hardened against attacks. Other types of software are less so.

Zoom makes the Web option difficult to find after clicking on the Join a Meeting link. In my testing on a Windows 10 machine, the option appeared only after I uninstalled the Zoom client. Even then, Zoom pushed an installation file after I tried to join a meeting. I was able to use the browser only after refusing the download and choosing Join from your browser. On a Mac, I was able to find the option, even when I had the Zoom client installed, by clicking cancel on the app installation dialog box. A Chrome extension called Zoom Redirector will also make it easy to find the link (Firefox and Edge versions of the open-source addon are here). The permissions required by the extension suggest it’s not much of a privacy or security threat.

Users opting for the browser option will have the best results if they use Chrome. Firefox and other browsers will prevent some key features, such as audio and video, from working at all. As a courtesy, meeting organizers can choose a setting that can make it easier for participants to find the option.

Fortunately, Zoom has disabled an attention-tracking feature that allowed organizers to tell when a participant didn’t have the meeting in focus for more than 30 seconds, for instance, because the participant switched to a different browser tab. This capability was intrusive. It’s great the Zoom removed it.

https://arstechnica.com/?p=1665450