The New York Times https://nyti.ms/39Sf3ns

How to Keep ‘Zoombombers’ Out of Your Meetings

There are a few steps you can take to make your video conferences more secure.

By Taylor Lorenz

April 7, 2020, 10:58 a.m. ET

As Zoom’s user base has grown in recent weeks, reports of “Zoombombing,” or “Zoom raiding,” have spread across the internet.

Public school classes, Alcoholics Anonymous meetings, yoga sessions and other virtual gatherings have been derailed by participants. Some of the these Zoombombers have been students, frustrated by online schooling and eager to escape the virtual classroom by any means. Others have weaponized the platform’s security flaws to harass specific populations using racial slurs, sexist remarks and pornography.

It’s nearly impossible to prevent these attacks, especially when an event is public by design (such as an A.A. meeting, or an open lecture). But there are a few steps you can take to make your meeting more secure.

Don’t share your Zoom link or code on social media

The easiest way to avoid getting Zoombombed is to keep your event private and your invite list small. If you are creating an event for a large, public audience, do not share your meeting link directly on social media. Instead, publicize an R.S.V.P. email address where people can state their interest in attending the event. That way, you can vet the list of prospective attendees and share the event link with only those whom you choose.

Set a meeting password

A meeting password — which is automatically generated by Zoom — will prevent uninvited users being able to join your event, even if they have the meeting link. Unfortunately, many Zoombombers swap and obtain meeting codes on social media. Be careful with where you share your meeting code, and if you can, wait to send it out until shortly before the event begins. *Read how to add a password here.*

Create a waiting room

A waiting room gives the meeting owner the ability to put everyone seeking to join the meeting in a virtual holding area. The host can then select only those whom they have invited to the meeting. Sometimes Zoombombers will use familiar names, so be careful to confirm the person's identity by asking them to turn their camera on. *Read how to create a waiting room here.*

Set screen sharing to "host only"

One popular way Zoombombers hijack a meeting is through the app's screen sharing function. When screen sharing privileges are set to "all," any member who joins a meeting could project offensive imagery to meeting's participants. *Read how to keep screen sharing privileges limited here.*

Turn off the annotation feature

Even if you limit screen sharing, trolls may draw offensive words or shapes over the host's presentation using the annotation tool, which gives users the ability to draw onscreen in different colors using a cursor. *Read how to restrict the annotation feature here.*

Restrict other features as needed in host controls

Zoombombers will leverage every feature they can to ruin a meeting. For some meetings it might make sense to block private chats, turn off file transfers and restrict custom backgrounds, all of which could be used to taunt or harass participants. *Read more on host controls here.*

Disable "allow removed participants to rejoin"

Trolls can be persistent. One way to thwart their efforts is by preventing them from rejoining. Unfortunately some attacks are coordinated, so there may still be other bad actors in your meeting, but at least you'll be one down. *Read how to disable the "allow removed participants to rejoin" option here.*

Make sure you're running the latest version of Zoom

Zoom recently announced that it would be shifting all engineering resources to combating harassment and improving security features in order to better protect users. "We are making sure if we get issues in terms of security, we update the client right away," said Oded

Gal, Zoom's chief product officer. "That's why it's important to update." *Read how to make sure you're using the latest version of the app.*

Taylor Lorenz is a technology reporter in New York covering internet culture. Before joining The Times, she was a technology and culture writer at The Atlantic and The Daily Beast. @taylorlorenz