How To Prevent "Zoombombing"

As the coronavirus pandemic has led to more people spending time at home and conducting school and business online, an increasing focus has been placed on certain technologies and their ability to facilitate hate and harassment. Reports of "Zoombombing," a reference to the popular video conferencing platform Zoom in which virtual meetings are disrupted by graphic or threatening messages or actions, often including those that contain hate speech or pornographic content, have quickly garnered attention across the country. Inside Higher Ed recently reported incidents targeting virtual classrooms at Arizona State University and the University of Southern California, as well as a children's storytelling session in New Jersey. According to NBC News, during a virtual Torah lesson on March 22, multiple people interrupted the session by sharing antisemitic images and language. In Thousand Oaks, California, an online school board meeting was cut short after someone shared pornographic images, as well as a Nazi flag and swastika.

While some of these reported Zoombombing incidents can be attributed to internet trolls without particularly malicious intentions, there is concern that extremists could exploit the increasing reliance on video conferencing technology to target certain groups or advance their hateful messages. Across various social media platforms, extremists have already seized on the coronavirus pandemic as a vehicle to spread their hate and conspiracies.

Staying safe when hosting Zoom meetings

Zoom Safety Checklist

Before Meeting:

- Disable autosaving chats

- Disable file transfer

- Disable screen sharing for non-hosts

- Disable remote control

- Disable annotations

- Use per-meeting ID, not personal ID

- Disable "Join Before Host"

- Enable "Waiting Room"

During Meeting:
- Assign at least two co-hosts

- Mute all participants

- Lock the meeting, if all attendees are present

If you are Zoombombed:
- Remove problematic users and disable their ability to rejoin when asked

- Lock the meeting to prevent additional Zoombombing

Instructions for how to perform all of these steps are included below.

While most meetings won't be Zoombombed, there are some safety measures that you can take when you host a Zoom meeting. [ADL's Center for Technology and Society](#) recommends the following:

When scheduling or setting up a meeting you will host:

Set Safe Meeting Default Settings

On the Zoom Settings page, turn off participant controls:

1. Sign into Zoom.us.

2. Click on the Settings link on the upper right (it looks like a gear).
3. On the right side of the page, **turn off:** Autosaving chats, file transfer, screen sharing, and remote control.

Assign a Co-Host

For larger meetings, identify a co-host or two ahead of time whose role is to be a virtual room monitor and manage order during the meeting by managing the participants. Co-hosts are assigned during a meeting and cannot start a meeting.

1. Sign into Zoom.us.

2. Click on the Settings link on the left of the screen.

3. Scroll down to the Co-host option on the Meeting tab and verify that the setting is enabled.

4. Turn on Co-Host. If a verification dialog displays, choose Turn On to verify the change.

Assign a per-meeting ID, don't use your Personal Meeting ID

Avoid using your Personal Meeting ID (PMI) to host public events. Your PMI is basically one continuous meeting - your personal virtual space; and once it is published, others can join at any time. Learn about meeting IDs and how to generate a random meeting ID (at the 0:27 mark) in this video tutorial.

Prevent Screen Sharing by non-hosts

To prevent participants from screen sharing during a call, use the host controls at the bottom of the window, click the arrow next to Share Screen and then choose Advanced Sharing Options.

- Under "Who can share?" choose "Only Host" and close the window. You can also lock the Screen Share by default for all of your meetings in your web settings.

Enable the Waiting Room

Before you start your meeting, enable the Waiting Room for your meeting. You and your co-host will then play an active role in choosing who to allow into the room through the participants list.

Meeting hosts can customize Waiting Room settings for additional control, and can even personalize the message that people see when they enter the Waiting Room so they know they're in the right spot. This is a great way to post rules and guidelines for your event, like your screensharing or muting policy.

Disable Join Before Host

Before starting a meeting, disable Join Before Host to keep users out before the host arrives. This is the current default, but double check to make sure that it is set for the meeting. When "Join Before Host" is enabled, anyone can enter at any time and create havoc with other participants before the meeting officially starts.

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 unsolicited pics, GIFs, memes, and other content.

Turn off annotation

You and your attendees can doodle and mark up content together using annotations during screen share. Disable the annotation feature in your Zoom settings to prevent people from writing all over the screens.

Once the meeting starts:

Manage Disruptive Participants

The Meeting Participants window offers control over most aspects of your meeting and those attending. Zoom has a 10 minute long video that is recommended viewing for all hosts and co-hosts.

Locking the Meeting to Prevent Re-Joining of Removed Participants

During the meeting, a host or co-host can click on the More and Mute All Controls at the bottom of the Participants List.

1. When viewing the Participants List, click Lock Meeting (under More) to prevent other participants from joining the meeting in progress.

Muting All Participants

During the meeting, a host or co-host can click on the More and Mute All Controls at the bottom of the Participants list.

1. On the Participants List, click Mute All to mute all meeting attendees.

More resources:

- How to Keep the Party Crashers from Crashing Your Zoom Event
- Zoom-bombing: How to keep trolls out of your Zoom meetings
- 'Zoombombing': When Video Conferences Go Wrong

https://www.adl.org/blog/how-to-prevent-zoombombing