Zoombombing: What it is and how you can prevent it in Zoom video chat

Video-conferencing software Zoom has been drawing attention from researchers and journalists lately for a number of potential privacy and security issues, as use of the platform surges due to an increase in coronavirus-related remote working.

One of the biggest security issues facing Zoom is the surge in "Zoombombing," when uninvited attendees break into and disrupt your meeting.

Similarly, rumors of security risks have circulated around other video-conferencing services. And the stakes are getting higher. Some have accused video-calling app Houseparty of enabling Netflix account hacks with loose security protocols. In response, the company has offered a $1 million reward for proof of security sabotage against what others argue is a viral misinformation campaign, saying that the problem is more likely tied to reusing login credentials and passwords.

On Thursday, Zoom CEO Eric Yuan responded to concerns, saying Zoom will freeze feature updates to address security issues, aiming to address them in the next 90 days.

It can be easy to Zoombomb a meeting. In many cases, a simple Google search for URLs that include "Zoom.us" can turn up the unprotected links of multiple meetings that anyone can jump into. Similarly, links to public meetings can be found scattered across organizational pages on social media.

While there are no guarantees against determined trolls, there are a few ways to hedge your bets and improve your overall privacy levels when using Zoom. Here's where you can start.

Zoom settings you should change now

There are some easy settings you can change before your Zoom meeting begins that will allow you to reduce the likelihood of intrusion by uninvited guests, and generally bolster your privacy overall.

1. Don't use your Personal Meeting ID for the meeting. Instead, use a per-meeting ID, exclusive to a single meeting. Zoom's support page offers a video walk-through on how to generate a random meeting ID for extra security.

2. Enable the "Waiting Room" feature so that you can see who is attempting to join the meeting before allowing them access. Like many other privacy functions, a skillful disrupter can sometimes bypass this control, but it helps to put another hurdle in their route to chaos.

Zoom offers a support article here as well. To enable the Waiting Room feature, go to **Account Management** > **Account Settings**. Click on **Meeting**, then click **Waiting Room** to enable the setting.

3. Disable other options, including the ability for others to **Join Before Host** (it should be disabled by default, but check to be sure -- see below). Then disable screen-sharing for nonhosts, and also the remote control function. Finally, disable all file transferring, annotations and the autosave feature for chats.

To disable most of these features, click on the gear-shaped **Settings** icon on the upper-right side of the page after you've logged in. From there, you'll see the option to turn off most of the listed features.

Disabling screen-sharing is a bit different, but just as easy. Go to the host controls at the bottom of your screen, and you'll see an arrow next to **Share Screen**. Click the arrow, then click **Advanced Sharing Options**. Go to **Who can share?** Click **Only Host**, then close the window.

4. Once the meeting begins and everyone is in, lock the meeting to outsiders (see our tips below) and assign at least two meeting co-hosts. The co-hosts will be able to help control the situation in case anyone bypasses your efforts and gets into the meeting.

To deputize your co-hosts, go to the same **Settings** icon, then to the **Meetings** tab. Scroll down to **Co-host** and make sure it is enabled. If Zoom asks you for verification, click **Turn On**.

What to do if someone Zoombombs your Zoom video chat

It happened. Despite your careful efforts of prevention, some jackal has gotten into the meeting to cause chaos for kicks. Short of ending the meeting entirely, here are a few things you can do to try and get rid of them.

1. Lock them out. Go to the **Participants List** in the navigation sidebar, and scroll down to **More**. Click **Lock Meeting** to stop further participants from entering the meeting and to be able to remove participants.

2. Shut them up. Have yourself or one of your co-hosts go to the **Participants List**, again scrolling down to the bottom, and click **Mute All Controls**. This makes it so the unwelcome participant can't use their microphone to disrupt your audio.

Good luck out there in the wide world of video chatting. For more advice on how to use Zoom, check out these tips for getting the most out of your video chat apps, and how to change your Zoom background.