SECURITY & PRIVACY

3 New Ways We're Combatting Meeting Disruptions

Matt Nagel
November 16, 2020 · 3 min read

Zoom released two new security features this weekend to remove and report disruptive meeting participants. We also wanted to share information about an internal tool we're using to help prevent meeting disruptions before they happen.

New security enhancements

Suspend Participant Activities

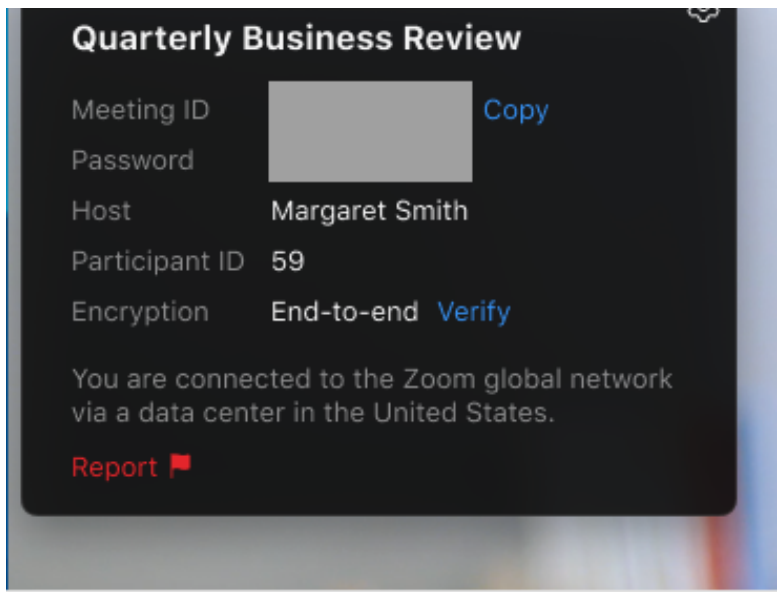
Under the Security icon, hosts and co-hosts now have the option to temporarily pause their meeting and remove a disruptive participant. By clicking "Suspend Participant Activities," all video, audio, in-meeting chat, annotation, screen sharing, and recording during that time will stop, and Breakout Rooms will end.

The hosts or co-host will be asked if they would like to report a user from their meeting, share any details, and optionally include a screenshot. Once they click "Submit," the reported user will be removed from their meeting, and Zoom's Trust & Safety team will be notified. Hosts and co-hosts may resume their meeting by individually re-enabling the features they'd like to use. Zoom will also send them an email after the meeting to gather more information.

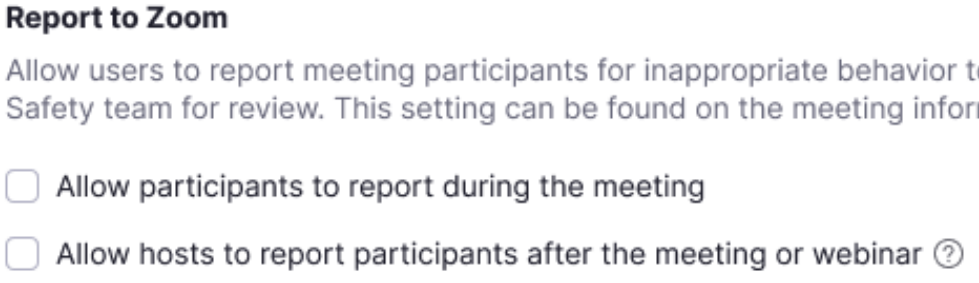
The Suspend Participant Activities feature is enabled by default for all free and paid Zoom users.

Report by Participants

Hosts and co-hosts can already report users from the Security icon, but now meeting participants can also report a disruptive user directly from the Zoom client by clicking the top-left Security badge.



Account owners and admins can enable reporting capabilities for non-hosts in their web settings.



Both of these new features are available on the Zoom desktop clients for Mac, PC, and Linux, and our mobile apps, with support for the web client and VDI to come later this year.

At-Risk Meeting Notifier

This fall, Zoom deployed an At-Risk Meeting Notifier to scan public social media posts and other websites for publicly shared Zoom Meeting links. When the tool detects a meeting that looks to be at high risk of being disrupted, it automatically alerts the account owner by email and provides advice on what to do. These steps could include deleting the vulnerable meeting and creating a new one with a new meeting ID, enabling security settings, or using another Zoom solution, like Zoom Video Webinars or OnZoom.

If you do get an email, it's critical to take action or risk having your meeting disrupted.

As a reminder – one of the best ways to keep your Zoom meeting secure is to **never share your meeting ID or passcode** on any public forum, including social media.

For more on our At-Risk Meeting Notifier, visit our support page. For additional tips on eliminating meeting disruptions, join one of our meeting security webinars.

Don't forget to share this post

You might also like

SECURITY & PRIVACY, ZOOMTOPIA

Zoom Rolling Out End-to-End Encryption Offering

Max Krohn
October 14, 2020 · 6 min read

EDUCATION, SECURITY & PRIVACY

Zoom SSO for the Classroom & the Benefits for Schools

Brendan Ittelson
October 7, 2020 · 2 min read

HOW TOS, SECURITY & PRIVACY

Security Tips for National Cybersecurity Awareness Month

Jason Lee
October 1, 2020 · 4 min read

Simplified video conferencing and messaging across any device

Request a demo

Buy now

OUR CUSTOMERS LOVE US

ZOOM IS RANKED #1 IN CUSTOMER REVIEWS

Copyright © 2020 Zoom Video Communications, Inc. All rights reserved. Privacy & Legal Policies | About Ads | Cookie Preferences | Do Not Sell My Personal Information