What Can You Tell me About Zoom?

BY THE MOZILLA TEAM | APRIL 3, 2020 | ADVOCACY

Zoom's popularity has taken off – just seven weeks into 2020, the company has seen more user growth than in all of 2019.

Here at Mozilla, we've been using Zoom for nearly a year at enterprise level. It allows our colleagues around the globe to connect with each other using high quality video and audio. When we were reviewing Zoom as a potential vendor, we asked a lot of questions about the platform's privacy and security protections, and we think it is good consumers are asking these types of questions now.

In our opinion, Zoom has done a solid job of responding to the questions, concerns, and interest that have come fast and furious in a short amount of time. Including:

- Recently researchers noted that Zoom's claim to enable end-to-end encryption was misleading – it is actually transport encryption – and that it's possible Zoom content could be accessed by the company itself. A day after that news broke, the company

apologized and published a post explaining how its encryption works.

- "Zoombombing," when malicious actors join a meeting to share inappropriate content, which has now become commonplace. As one researcher points out "Zoombombing" is networked harassment, but Zoom has security features readily available that can help prevent someone from hijacking your Zoom gathering (**for more, see our post on Zoom tips here.**)
- Investigative reporters at Motherboard recently reported that the iOS Zoom app was sharing data with Facebook – but within a day of the story breaking, Zoom responded with an app update to fix the bug and stop sending data to Facebook.
- The company affirms that it does not sell user data, and recently updated its privacy policy to make it clearer what data they collect and how it is used, including explicitly clarifying that it does not sell users' data.
- Zoom's "attention tracking" feature, which let hosts know if participants have a window other than Zoom in focus for more than thirty seconds during screen sharing, drew some attention, too. To Zoom's credit, the company disabled this feature on April 1.

Another question that has arisen recently is about Zoom and telemedicine. Zoom says it is set-up for HIPAA compliance, *with its healthcare provider customers;* that doesn't mean your particular provider is part of Zoom's program. So be careful to check that your healthcare provider has the correct plan, and do not assume that if

you invite your healthcare provider to a Zoom call, that the HIPAA security protections are in place by default. Be sure to educate yourself. As Consumer Reports notes, many of those new to the platform – or even people who have been using it for years – may not understand the privacy implications of Zoom or other video conferencing tools.

We are gratified to know, and see through its actions, that Zoom is committed to putting privacy and security first, and we are working closely with the company to make sure it continues to do so. As with all of our advocacy work, we will continue to keep an eye on the situation and press for necessary changes to protect your privacy.

Protect the internet as a global public resource

Join our **Mozilla News** email list to take action and stay updated!

Please enter your email

Sign up

I'm okay with Mozilla handling my info as explained in this Privacy Notice

More about us

Donate

Legal

License

Participation Guidelines

Privacy

Cookies

Language English

Mozilla is a global non-profit dedicated to putting you in control of your online experience and shaping the future of the web for the public good. Visit us at foundation.mozilla.org