

Our First ‘Ask Eric Anything’ Webinar Addresses Users’ Security & Privacy Concerns

APRIL 8, 2020 BY [ZOOM](#)



Zoom founder and CEO Eric S. Yuan kicked off his weekly “Ask Eric Anything” webinar today as part of [our commitment](#) to creating the best and safest Zoom meeting experiences for our users. Eric plans to use this platform over the next 90 days to address security, privacy, data, and any other concerns from Zoom users, and we’ll share highlights from each of his sessions.

Speaking to more than 5,900 attendees on the webinar and many more joining via the YouTube livestream, Eric reiterated Zoom’s commitment to helping our users stay connected during this time and also our efforts to “double down” on privacy and security.

Here are some of the specific questions Eric answered during this week’s session:

How can we prevent unwanted participants from dropping in on our meetings?

“First of all, every meeting should have a password. And ideally, only use your personal meeting ID for internal meetings. Otherwise, use a randomly generated meeting ID. The Waiting Room is also great for security, especially for K-12 schools. For business meetings, I normally use a password, and after everyone has joined, I lock the meeting. And for very sensitive meetings, I will only allow authenticated users from the same domain as mine to join the meeting.”

What are your plans for Zoom's encryption?

"Today, the way we use AES encryption, the key is generated by our system. And we're working on a feature so that the key will be generated from you, from our customers. We're upgrading our encryption from AES-256 ECB to AES-256 GCM. We've already enabled that for one customer, and over the next several months, we are going to roll this feature out to all of our customers. However, every client needs to be updated to the latest version to work so that may take some time. So I think that will be a focus over the next 45 days."

Does Zoom ever provide user data to other companies or entities?

"To process our online payments, we needed to use a third-party billing engine. Other than that, we never share any user data from meetings. The only data that we use internally from those meetings in the metadata, or the data about the performance of the meeting. This helps us with analytics and improving the meeting experience. ... But selling data has never been part of our business model."

Is Zoom safe to use for telehealth? Is Zoom HIPAA compliant?

"Yes, we've supported HIPAA clients for some time. Telemedicine is really important, and we've doubled down on that. We have a lot of healthcare organizations using Zoom during this pandemic. We can also set BAA (Business Associate Agreements) with healthcare customers, and we have integrations with other healthcare systems like Epic."

Has file sharing been disabled, and if so, when will it be available again?

"All of our resources are focused on looking in every corner, looking at every line of code, looking at every feature to make sure there aren't any security or privacy issues, and we found a potential security vulnerability with file sharing, so we disabled that feature. If there is any conflict between our features and our user's privacy and security, privacy and security come first."

Thanks to everyone who attended and engaged with us during this "Ask Eric Anything" session. We hope it was helpful, and we invite you to share feedback on today's session by emailing answers@zoom.us.

And in case you missed it, you can watch the recording:

You can also sign up for next week's webinar — and get your Zoom questions answered — [here](#).

ANNOUNCEMENTS EXECUTIVE INSIGHTS