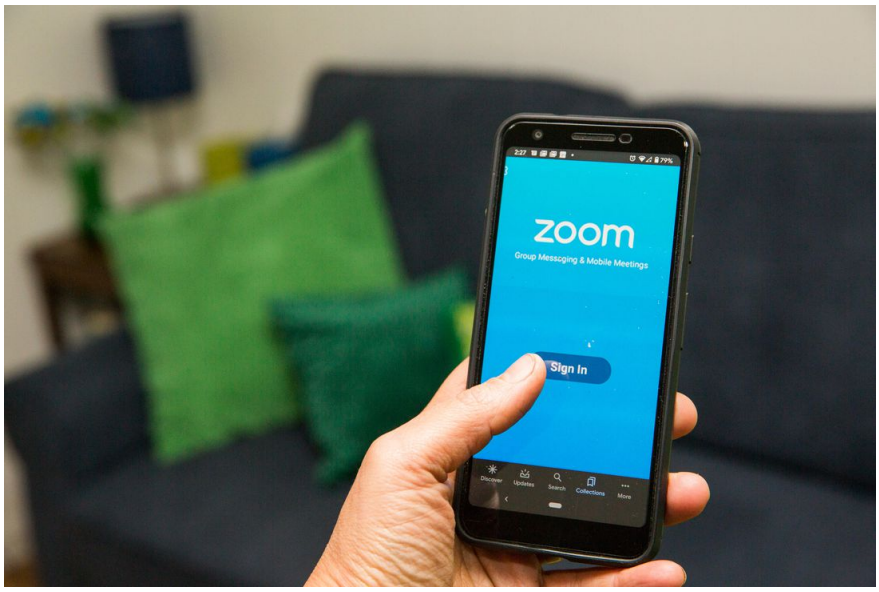
Using Zoom while working from home? Here are the privacy risks to watch out for

Don't let tattle-tale software features disrupt your remote workflow.

Now that you've finished choosing your custom Zoom background, mercifully sparing your fellow workers-from-home the sight of a growing pile of gym socks behind your desk, you might think you've got a handle on the conference call software du jour. Unfortunately, there are a few other data security considerations to make if you want to hide your dirty laundry.



Privacy experts have previously expressed concerns about Zoom: In 2019, the video-conferencing software experienced both a webcam hacking scandal, and a bug that allowed snooping users to potentially join video meetings they hadn't been invited to. This month, the Electronic Frontier Foundation cautioned users working from home about the software's onboard privacy features.

With the novel coronavirus causing a surge in work-from-home activity, Zoom has quickly become the video meeting app of choice. And with that popularity, privacy risks are extending to a greater number of users.

Here are some of the privacy vulnerabilities in Zoom that you should watch out for while working remotely.

Tattle-tale

Employers, managers and workers-from-home, beware. Zoom's tattle-tale attention-tracking feature can tell your meeting host if you aren't paying attention to their meticulously-composed visual aids. Whether you're using Zoom's desktop client or mobile app, a meeting host can enable a built-in option which alerts them if any attendees go more than 30 seconds without Zoom being in focus on their screen.

If you're anything like me, your Zoom meetings rarely consume your full screen. Jotting down notes in a separate text file, adding dates to calendars, glancing at reference documents or discreetly asking and answering clarifying questions in a separate chat -- these key parts of any normal meeting are all indicators of an engaged listener. When translated to online conferencing, they often mean switching windows and shouldn't be mistaken for signs of inattention.

To shore up your privacy, though, consider switching to a separate device if you want to handle secondary meeting tasks or make memes about poorly constructed pie charts.

Cloud snitching

For paid subscribers, Zoom's cloud recording feature can either be a life-saver or a catastrophic faux pas waiting to happen. If the feature is enabled on the account, a host can record the meeting along with its text transcription and a text file of any active chats in that meeting, and save it to the cloud where it can later be accessed by other authorized users at your company, including people who may have never attended the meeting in question. Yikes.

As Mashable's Zack Morse put it, "What that suggests, but doesn't clarify, is that for non-webinar/standard meetings, your person-to-person chat messages would be later sent to your boss after a call recorded to the cloud."

Zoom does allow a narrowing of the audience here, however. Administrators can limit the recording's accessibility to only certain preapproved IP addresses, even if the recording has already been shared.

Data gossip

By now, you're used to hearing it from the privacy-minded: Don't use Facebook to log in to other sites and software unless you want Facebook to have data on what you're doing. Fair enough. But what to do when Zoom gets caught sending some of your analytics data to Facebook -- whether or not you even have a Facebook account?

An analysis by Vice's Motherboard, published Thursday, found the iOS version of the Zoom app doing exactly that. Courtesy of Facebook's Graph API, Zoom was telling Facebook whenever you opened the Zoom app, what phone or device you were using, and your phone carrier, location and a unique advertising identifier. Late Friday, Motherboard reported that Zoom had updated its iOS app so the app would stop sending certain data to Facebook.

Zoom didn't respond to CNET's request for comment. But in a statement to Motherborad on Friday, it said the following:

"Zoom takes its users' privacy extremely seriously. We originally implemented the 'Login with Facebook' feature using the Facebook SDK in order to provide our users with another convenient way to access our platform. However, we were recently made aware that the Facebook SDK was collecting unnecessary device data."

The breezy language in Zoom's privacy policy about its relationship to third-party data crunchers gives one reason to question where else -- and to what extent -- that data is being shared or sold that we don't know about.

"Zoom does use certain standard advertising tools which require Personal Data (think, for example, Google Ads and Google Analytics). We use these tools to help us improve your advertising experience (such as serving advertisements on our behalf across the Internet, serving personalized ads on our website, and providing analytics services)," the policy says. "Sharing Personal Data with the third-party provider while using these tools may fall within the extremely broad definition of the 'sale' of Personal Data under certain state laws because those companies might use Personal Data for their own business purposes, as well as Zoom's purposes."

Here's a summation of the above corporate jargon: Zoom shares data with enough advertisers and data crunchers, in enough states, that it would broadly qualify as selling your data.

You should probably review your Zoom and device security settings with an eye toward minimizing permissions, and make sure any antitracking software on your device is up to date and running.

It may not help, but it can't hurt.