
ZOOM PRIVACY AND SECURITY

TO: Domestic Violence Support Service (DVSS) Providers

FROM: Angela Boger, Program Director, Domestic Violence Housing & Support Services (DVHSS)

SUBJECT: Service Provision During COVID-19 Pandemic

DATE: 4/13/2020 9:58 AM

CC: Ellen Eidem, Zoe Phillips, Laurle'ta Williams, Clarynda Ogwuka, Myshal'e Oliver, Martha Chono-Helsley, Yeira Rodriguez, Kang Nong Liang, Dara Kaing, Carol Chow

Good Morning,

Hoping you all are well. With millions of people currently physically distancing at home, Zoom has become an easy and accessible communication tool. Many agencies also find it a preferable application for interfacing with staff and coworkers. However, Zoom has significant **privacy and security flaws** that DV agencies must consider.

In the past few weeks, Zoom has come under scrutiny for several violations of security and privacy including:

- Leaking information to social media
- Susceptibility to eavesdropping (no end-to-end encryption of communication)
- Local privilege escalation (happens when one user acquires the system rights of another user)
- Threat actors taking over Zoom sessions and secretly activating cameras

Please do not use Zoom for domestic violence client work including one-on-one and group sessions.

Zoom's security is fine for general staff meetings. However **since the provision of client services are sensitive**, you should know that the platform's [claims of end-to-end encryption don't hold up](#), and critics have found that the type of encryption it implements are lacking in some ways.

Although we do not recommend using Zoom for the provision of group services, there are some settings you can use to make Zoom a **safer** place for your staff.

1. **Stop Zoombombs** - If your Zoom meeting ID # becomes public somehow, or trolls find it in a web search or guess it, they can pop into your chats and disrupt them. **Be careful with sharing the meeting ID with unknown participants.** Keep in mind that contacts you've added in Zoom will be able to see your Personal Meeting ID.
2. **Enable Waiting Room** by going to your [Zoom settings](#) on the web under “**Advanced Options for Hosting Meetings.**” This step allows for people calling in to be on hold before you give them specific approval to join.
3. **Restrict Users** - Go to your [Zoom settings](#) on the web and click “**In Meeting (Basic)**”, you'll see a “**Screen Sharing**” option. This setting will stop anyone except you from sharing the desktops or apps on their computer. You can still grant screen sharing privileges to specific users in a meeting later, if you need to.
4. **Lock Meeting** - Lock a meeting once you're sure that everyone who needs to join the meeting has joined. From the [Desktop app](#), click “**Manage Participants**”, “**More**”, and then “**Lock Meeting**”. Just make sure that you weren't expecting someone who hasn't yet arrived, as they won't be able to get in. **To absolutely lock down a meeting, make sure participants have a password to access it.**
5. **Try an Alternative** – Here are some suggestions (not endorsed by LA County) for other platforms that have more robust encryption in place below.
 - [Google Duo](#): maximum video chat group size from 8 to 12, it's available on mobile devices and the web, and video and audio calls are end-to-end encrypted.
 - [Webex from Cisco](#) is a group video calling tool that supports end-to-end encryption and supports video calls of up to 100 people.
 - [GoToMeeting](#) includes end-to-end encryption as a standard. Unlike Webex, there are no free plans, so your company will have to pay \$12 a month and up for video calls with up to 150 different people. There's also a 14-day free trial.

If you use Zoom for your personal use here is an article that can help you understand how to make using it more secure, [Wired Magazine](#).

Angela Boger, Program Director
Department of Public Health, Office of Women's Health
Domestic Violence Housing and Support Services Unit