SĀGIN, LLC

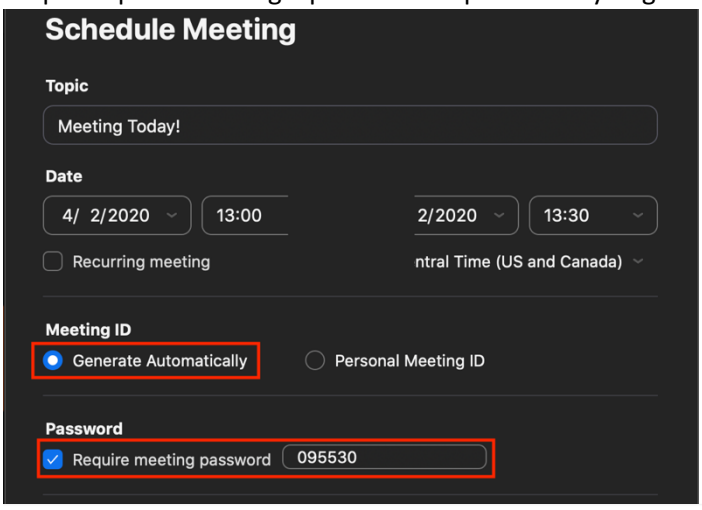
Protecting Yourself From Zoom-bombing

As our work, school, and social interaction has increasingly moved online in the wake of COVID-19, a new security issue known as Zoom-bombing is becoming increasingly common. Zoom-bombing is named as such for the way uninvited participants jump into in-progress Zoom meetings and hijack them, and attacks reported thus far have resulted in meetings being derailed with pornographic content and hate speech.

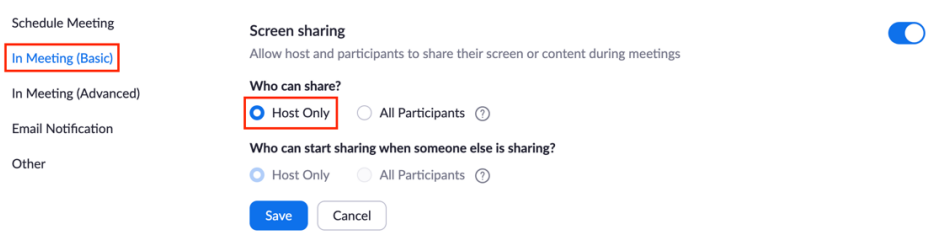
Zoom-bombing has arisen as Zoom downloads in Illinois alone topped 2.29 million in March 2020, up from just 171,574 in January 2020 according to the Chicago Tribune. It is relatively easy for hijackers to pull off due to common meeting defaults used by Zoom. Below are some steps you can take to prevent your Zoom meetings from being hijacked by bad actors and keep up productivity, both within the Zoom app when setting up your meeting and in your personal account settings accessible within the Zoom Web Portal (https://zoom.us).

Use a Unique Meeting ID *Instead* of Your Personal Meeting ID (Zoom App)
Your Personal Meeting ID is convenient to use, but it's also an easy way for uninvited guests to crash your meetings. Once your Personal Meeting ID is public, it stays public and can let anyone join uninvited. Instead, have Zoom generate a unique ID – this is especially important for publicly advertised events. To do this, when you schedule a meeting be sure **Generate Automatically** Under **Meeting ID** is selected.

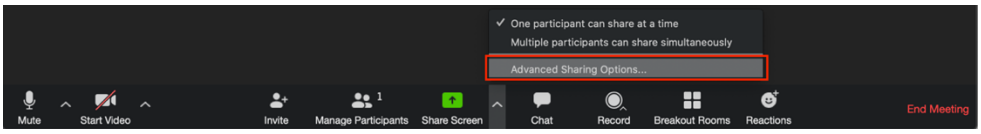
Secure your Meeting by requiring a Meeting Password (Zoom App)
In particular for meetings that you wish to post publicly, but only have those you wish join, require a meeting password for participants. Setting a password requires that you generate an automatic Meeting ID.

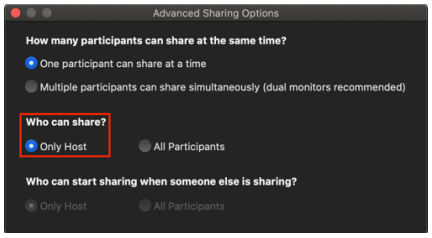


Allow Only Hosts to Share their screen (Zoom Web Portal)
Using this setting will prevent any bad actors (or someone not paying attention) from hijacking your meeting by displaying their screen. To do so before your meeting begins, head to your Personal Settings on the **Zoom Web Portal** and navigate to **In Meeting (Basic)** → **Screen Sharing**. Set **Who Can Share** to **Host Only** and be sure to click **Save**.



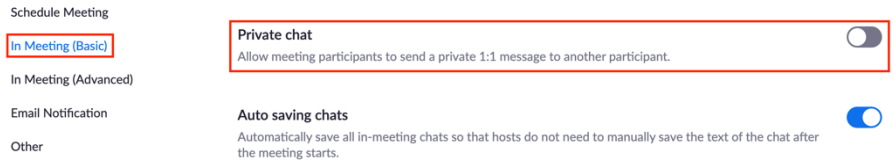
If your meeting has already started, you can change this setting from the meeting controls by clicking the carrot **^** next to **Share Screen → Advanced Options**. Set **Who can share?** To **Only Host**.



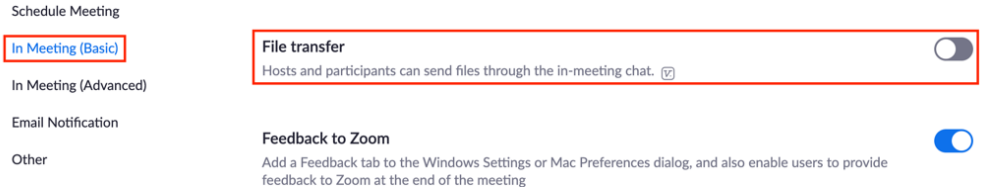


Disable In-Meeting Private Chat and File Transfers (Zoom Web Portal)

You can prevent your participants from one-on-one chatting each other during the meeting. This is most useful if you have strangers attending your meeting to prevent potential harassment of guests. In the Zoom Web Portal, navigate to **Personal Settings → In Meeting (Basic) → Private Chat** and toggle the slider to **Off**.

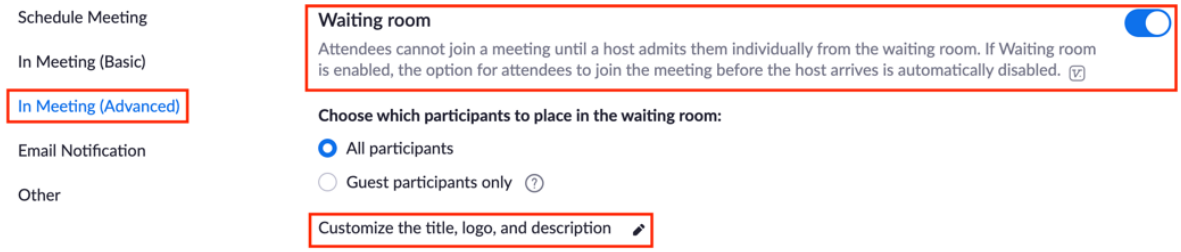


Similarly useful for public events, you can prevent participants from sharing files to the group chat. This is located in **Personal Settings → In Meeting (Basic) → File Transfer** and toggle the slider to **Off**.



Use the Waiting Room Function (Zoom Web Portal)

Beyond an automatically generated Meeting ID and a meeting password, using a Waiting Room will prevent the meeting from starting before the host joins. This option lets you screen participants before they join, or you can let all participants in at the same time. As a side benefit, you can customize your Waiting Room's title, logo, and description to your business's branding. You can access this before your meeting starts by going into your **Personal Settings → In Meeting (Advanced)** → Toggle the slider for **Waiting Room**.



Using these settings will help you keep your Zoom meetings safer and more productive, whether they be for your weekly team huddle or a larger event. Beyond following these recommendations, be sure to keep up with announcements from the services you use about feature changes and security updates. This will help ensure you are always in the know about what is changing and can adapt to meet new challenges.