Secure your zoom Meeting

Why so secure?

In recent weeks, with the massive nationwide shift from in person to online communication and collaboration, organizations throughout the country including government entities, education institutions, and private sector organizations have experienced what has now been coined as "Zoombombing". "Zoombombing" is the practice of bad actors joining Zoom meetings to share racist, misogynistic, and/or vulgar content via both screen sharing and chat communications.

The good new is, every Zoom host can take large steps to prevent this scenario by adjusting their settings and in meeting host controls to enhance the security of the Zoom client and keep these bad actors at bay.

The steps listed below are *necessary* to enhance the security of your Zoom meetings and to ensure you remain secure and in control.

What can you do?

Are you a Participant?

1. *Make updating your Zoom client a habit.*
You can check for updates anytime by logging into your Zoom desktop application, clicking on your profile photo (or initials) and selecting Check for Updates from the drop down list.

2. Use two devices during your Zoom calls. For example, use your phone to check emails or chat with other call attendees.

Are you a Host?

Both steps 1 and 2 above and:

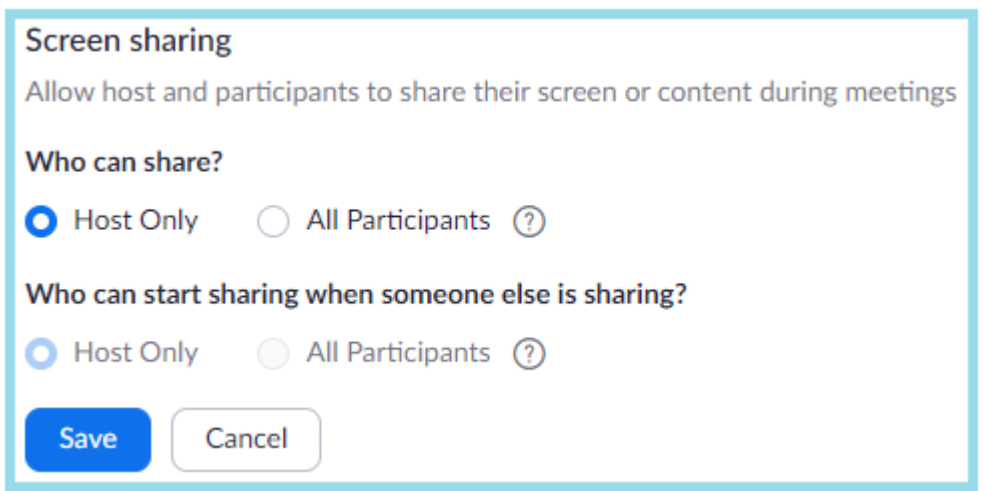
3. Click on MY ACCOUNT in the upper right corner of your Zoom dashboard.

4. Then, select your Zoom Settings located on the left hand side of the screen and do the following:

→ **Disable File Transfer**

→ **Limit Screen Sharing to Host Only**

Don't forget to save!



tech tip!
You will know that the setting is disabled when the slider turns gray.

Enabled features will show as a blue slider.

→ **Disable Annotation**

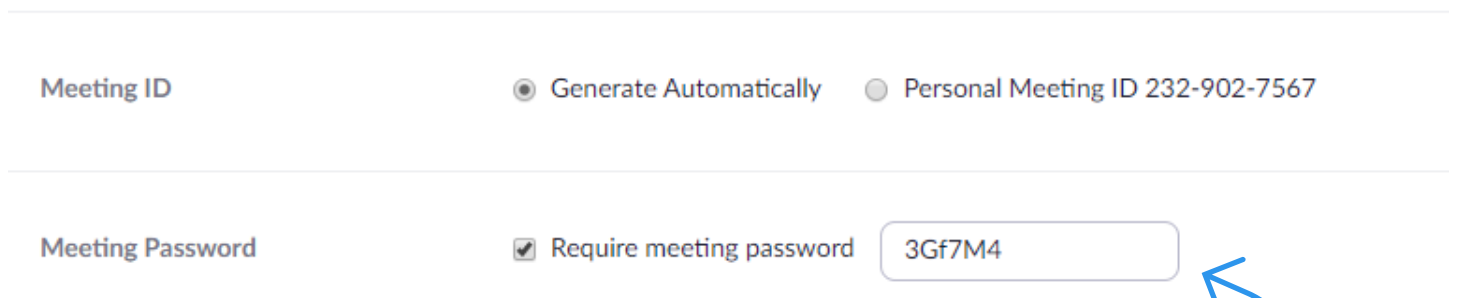
→ **Disable Allow removed participants to rejoin**

→ **Enable the Waiting Room**

5. Once these settings are configured, you are ready to book your meeting. Click SCHEDULE A MEETING and update the following settings.

→ **Set your meeting ID to Generate Automatically**

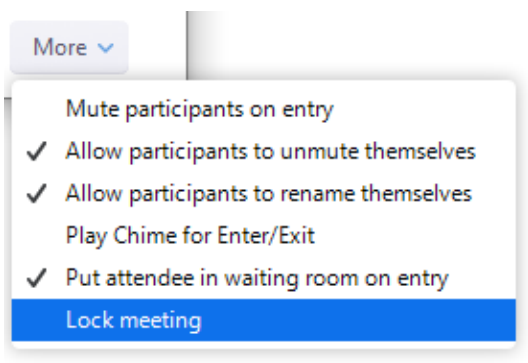
→ **Mandate a meeting password**



tech tip!
Set a new password for each meeting you host.

→ **Deselect** Enable join before host

6. Once your meeting has started, lock-down your meeting to uninvited guests by selecting "More", "Lock meeting" in the lower right of the participant pane.



What additional measures can you take?

- *Never* post any links to join meetings on the web, social media, or through a mass distribution list. Provide the link directly to the specific people who need to attend the meeting.
- Do not allow single sign-on with social media accounts. Login must be through a password.
- Create a strong password for each meeting. Change the meeting password for each meeting you host.
- Do not use your personal meeting ID for any business meeting.