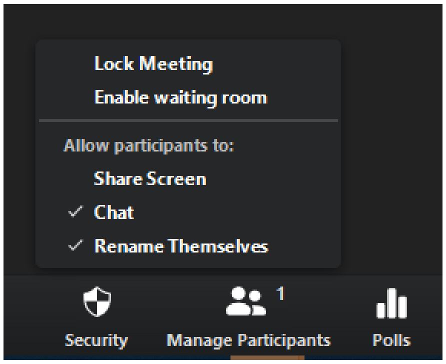
Zoom Video Conferencing

Best Practices – MEETING SECURITY for Hosts

v.3.0

Sadly, with the increased use of video conferencing there has been an increase in bad behavior by malicious participants (Zoom-bombing). Recent news stories report some meetings, including church events, being disrupted or shut down because a participant intentionally “hijacked” the meeting with inappropriate content.

Zoom has made several changes to prevent such behavior -- including defaulting to requiring meeting passwords and making the security settings more visible on the host’s screen -- but it is ultimately up to the host to set up and configure the meeting properly. You must have the latest Zoom client installed to see the new Security controls on PCs and Macs. For mobile devices see More > Meeting Settings.



Lock Meeting
Enable waiting room
Allow participants to:
Share Screen
✓ Chat
✓ Rename Themselves

If you send your meeting invitations to a group of people *known to you or to your organization* via text or email, you are probably not at risk.

You could also post the meeting ID publicly and send the password privately. The full meeting link *can* include the password. See Enabling Passwords.

If you post your meeting links publicly on a website or on social media, become familiar with:

In-meeting Security Options

Definitely:

Turn off participant screen sharing – the host can turn on screen sharing for participants as needed – (in meeting) Security > Share Screen or Share Screen > Advanced Options.

You can also:

Turn off virtual backgrounds (if enabled)

See: Virtual Background (on web portal) Personal > Settings > Virtual…

Turn off in-meeting file transfer (if enabled) **–** Never download or open a file unless you know what is included **and** you trust the sender.

See: In-Meeting File Transfer

Turn off Whiteboard sharing (on web portal) Settings > In Meetings (Basic) > Whiteboard.

Remember:

To avoid issues with noise, feedback, background conversations…

Mute all participants when joining – and decide if participants can unmute themselves or not.

See: Mute All and Unmute All or change the setting when scheduling.

Rev. Dr. Von Clemans, April 11, 2020