Zoom Video Conferencing

Best Practices – MEETING SECURITY

Sadly, with the increased use of video conferencing there has been an increase in bad behavior by malicious participants (Zoombombing). Recent news stories report some meetings having to shut down because a participant intentionally “hijacked” the meeting with inappropriate content.

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.

If you post your meeting links publicly on a website or on social media, consider the following adjustments to your meeting settings prior to or during your meeting…

Definitely:

Turn off participant screen sharing – the host can turn on screen sharing for individual participants as needed.
See: Managing participants in a meeting (Share Screen > Advanced…)

Consider:

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

Also:

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 setting when scheduling

Rev. Dr. Von Clemans, March 24, 2020