Zoom Settings

On our call there was a question about if hackers can access your zoom calls and how to prevent that challenge through settings. This is what I found, but have not tested. Plus a few extra notes.

Here is snippits from a Fortune article about Zoom Bombing - Hackers gain access to a Zoom meeting and attempt to disrupt the video chat and upset participants by shouting profanity or racial slurs, or putting disturbing or offensive images in their video feed.

Zoom users should not share meeting links publicly. This is perhaps the single most obvious precaution you can take. Rather than posting a meeting link to a Facebook group or in a promotional tweet, distribute information via a more private method, such as email.

Set your meetings to "private." Zoom now sets all new meetings to "private" by default, requiring attendees to provide a password for access. But users often opt to make meetings public for the sake of convenience.

Don't use your personal meeting ID. Every registered Zoom user has a personal meeting ID, linked to what is essentially a permanent virtual meeting room. Because that ID doesn't change, sharing it publicly increases the chance that future meetings using your personal ID might be Zoom bombed.

Restrict video sharing. If the meeting host is the only person who needs to share video, such as in a seminar or presentation, the host should change Zoom's screen-sharing setting to "Host only."

Full Article.

https://fortune.com/2020/04/02/zoom-bombing-what-is-meeting-hacked-how-to-prevent-vulnerability-is-zoom-safe-video-chats/

7 Zoom Tricks Article

https://www.fastcompany.com/90483200/ive-been-doing-zoom-meetings-for-years-these-7-tricks-make-them-great