Rotary District 6440

Zoom Meeting Security

Like much of the world, most Rotary District 6440 clubs have transitioned to meeting virtually, many with the Zoom meeting system. With so many people and groups using the system, it is not surprising that bad-actors are now crashing meetings to spread propaganda and hate messages or just cause mischief. Other bad-actors are looking for ways to learn private information about users that they can use in criminal activity and scams.

Zoom is taking this issue seriously and has devoted all of its development resources to enhancing the systems security features. All registered users can expect regular email updates from Zoom (the first came Friday April 3) and app updates.

We anticipate that Zoom's security settings and recommended protocols will be changing, and the District Virtual Meeting Committee will keep our clubs' Virtual Meeting Coordinators updated.

Going forward, all Zoom meetings will require passwords. At this time, this feature cannot be disabled.

Also, the default setting for accounts is now to require meeting attendees to go to a waiting room before entering a meeting, and the meeting host must permit attendees to enter the meeting. This feature can be disabled.

There are several steps you should take to ensure a secure environment for yourself and your club. There are other optional steps you can take to enhance security, depending on the degree of threat you and your club perceive.

Security Steps Everyone Should Adopt Now

1. Make sure you have the most current version of the Zoom app on all devices you use to connect to meetings.
2. When signing in to Zoom, do not use the “Sign in with Facebook” or “Sign in with Google” features.
3. Do not post Zoom meeting links to social media or websites or other publicly available places, unless you are welcoming everyone to attend, including potential bad actors.

4. If you do post links to public places, do not include the meeting password in the link.
    - You might adopt a common “easy to remember/hard to guess” password to be used for all meetings of your club.
5. If you are hosting meetings, know how to quickly mute all attendees and remove an attendee from a meeting. This process is a bit different on different devices, so be sure you know how on your device type.

Other Security Measures

1. Use a different randomly generated Meeting ID for all meetings. This means not scheduling recurring meetings, as they use the same Meeting ID for all occasions.
2. Only allow the host or cohost to share during meetings.
3. Have attendees hold in a waiting room until the host is ready to let them in the meeting. You can admit attendees 1 by 1, or admit them all at once. This allows the host to explicitly approve attendees who can join a meeting. Note, this is now the default setting for most accounts.
4. Require attendees to pre-register for meetings. This will also allow meeting hosts to get reports of who attended.
5. Disable the Annotation feature which allows attendees to annotate over shared screens or white boards.
6. Do not allow joining meetings by telephone or record meetings, as these disable Zooms encryption process and make your meeting content or video more susceptible to hacking attempts.

Note, while the above actions will enhance the security of your meetings, they will make it more difficult for people to join your meetings and/or limit the functionality and utility of meetings. Choose which security measures to adopt based on your meeting’s security needs and your perception of your security threat environment.