Rotary | ROTARY CONNECTS THE WORLD

Zoom seems to be the tool of choice for virtual connections during the COVID-19 pandemic. Usage has gone from 10 million in December, 2019 to 200 million in March, 2020. There have been in-meeting security issues for a few, mostly resulting from users making security choices that leave their connections vulnerable. These are recommended best practices for making your meetings safe and pleasant:

1. PASSWORD PROTECT YOUR MEETINGS

The simplest way to prevent unwanted attendees and hijacking is to set a password for your meeting To set up a password at the individual meeting level, head straight over to the "Settings" tab and enable "Require a password when scheduling new meetings", which will ensure a password will be generated when a meeting is scheduled. All participants require the password to join the meeting. **The password will be embedded in the link that is generated for your invitation**, so as long as users have the link, they will be able to enter the meeting. A numerical password is included in the invitation message for those connecting by phone.

2. JOIN BEFORE HOST

Do not allow others to join a meeting before you, as the host, have arrived. You can enforce this setting for a group under "Account Settings”, or set it when you are setting up the meeting.

3. TURN OFF PARTICIPANT SCREEN SHARING

No-one wants to see unsavory material shared by a Zoom bomber, and so disabling the ability for meeting attendees to share their screens is worthwhile. This option can be accessed from the new "Security" tab in active sessions.

4. USE WAITING ROOMS

The Waiting Room feature is a way to screen participants before they are allowed to enter a meeting. While legitimately useful for purposes including interviews or virtual office hours, this also gives hosts greater control over session security.

Thank you to our virtual clubs for their flexibility as we all navigate the new world of virtual Rotary meetings.