ROC # 141249

AV INNOVATIONS INC.

AVIoT Systems Integrator
4408 E Speedway Blvd, Tucson, AZ
Off: (520) 325-4206 Fax: (520) 327-8773
www.avinnovations.com

Secure Your Next Zoom Meeting

As millions of people look to Zoom as a go-to source of video and audio conferencing, it's essential to keep your meetings safe and secure. We highlight a few best practices to make sure your meetings are secure before, during, and after.

10 ways to enhance your meeting security.

1. Use a unique ID for large or "public" calls
   When you schedule a Zoom meeting, look for the Meeting ID Options, and choose Generate Automatically. Doing so can plug up one of the most significant holes hackers can exploit.

2. Create an invite-only meeting
   This might seem juvenile, but when the meeting is invite-only, the participants must sign in with the email address you used to invite them.

3. Require a meeting password
   Implementing a password can increase your Zoom meeting safety ten-fold. Give the password out only to those who are reliable, credible, and should be attending the call. To protect your meeting with a password, schedule a meeting, and check the box next to "require meeting password." Update: As of 5 April, 2020; scheduled meetings will have Passwords Enabled – if your attendees are joining via a meeting link, there will be no change. For those joining a meeting by manually entering a Meeting ID, they will need to enter a password to access the meeting

4. Create a waiting room
   When participants log into the call, they will be directed into the virtual waiting room. This gives the host an opportunity to let people into the call manually or accept all attendees at once. This process allows the host to decline access to names they do not recognize. Update: As of 5 April, 2020; the virtual waiting room will be automatically turned on by default.

5. Lock a meeting once it begins
   When the Zoom meeting beings, navigate to the bottom of the screen and click Manage Participants. The participants panel will open and at the bottom click More > Lock Meeting.

6. Only the hosts should share their screen
   Make sure the Zoom call settings are set to allow only the hosts to share their screen. You can set this up in advance or even during the call. Create a co-host to help with the meeting.

7. Kick someone out or put them on hold
   If a participant is questionable, go to the Participant Panel and hover over the name of the person you would want to boot or place on hold. Options will appear, choose Remove.

8. Disable someone's camera
   If you need to allow participants to share their screen, that is perfectly OK. But, if a participant is rude or inappropriate while on the video chat, the host can open the Participant Panel and click on the video icon next to the person's name. This will deactivate their camera

9. Prevent animated GIFs and other files in the chat
   Participants can share these items in the chat, unless the meeting is set up not to allow these items.

10. Disable private chat
    To do this, open Settings in the Zoom Web Application (it's not available on the desktop app). Go to Personal > Settings, then click in Meeting (Basic). Scroll until you see Private Chat and make sure the button is disabled.

To learn more about Hosting a secure Zoom Meeting: go to www.support.zoom.us For additional information on videoconferencing & presentation solutions for conference rooms and remote worker call or email us at Support@avinnovations.com