Best practices for remote conferencing

*Topic – WebEx Tips*

*Paulo Vasconcelos - Chair*
Best practices for remote conferencing

Membership Development - Training Topic

1. Use a Unique ID for Large or Public Zoom Calls
   - When you schedule a Zoom meeting, look for the Meeting ID options and choose Generate Automatically. Doing so plugs up one of the biggest holes that Zoom-bombers can exploit.

2. Require a Meeting Password
   - One way to protect the meeting is to require a password. You can give the password out only to those who have replied and seem credible. To password-protect a meeting, start by scheduling a meeting and checking the box next to Require meeting password.

3. Create a Waiting Room
   - When participants log into the call, they see a Waiting Room screen, the host, lets them in. You can let people in all at once or one at a time, which means if you see names you don’t recognize in the Waiting Room, you don’t have to let them in at all.

4. Only the Hosts Should Share Their Screen
   - Make sure your settings indicate that the only people allowed to share their screens are hosts. You can enable this setting in advance as well as during a call.

5. Create an Invite-Only Meeting
   - Only people who can join the call are those you invited, and they must sign in using the same email address you used to invite them.

6. Lock a Meeting Once It Starts
   - While the meeting is running, navigate to the bottom of the screen and click Manage Participants. The Participants panel will open. At the bottom, choose More > Lock Meeting.

7. Kick Someone Out or Put Them on Hold
   - During the call, go to the participants pane on the right. Hover over the name of the person you want to boot and when options appear, choose Remove.

8. Disable Someone’s Camera
   - If someone is being rude or inappropriate on video, the host can open the Participants panel and click on the video camera icon next to the person’s name.

9. Prevent Animated GIFs and Other Files in the Chat
   - In the chat area of a Zoom meeting, participants can share files, including images and animated GIFs—if you let them.

10. Disable Private Chat
    - Open Settings in the Zoom web app (it’s not in the desktop app). On the left side, go to Personal > Settings. Then click in Meeting (Basic). Scroll until you see Private chat. When the button is gray, it’s disabled.

Info credit: [https://www.pcmag.com/how-to/how-to-prevent-zoom-bombing](https://www.pcmag.com/how-to/how-to-prevent-zoom-bombing)

Design: Liberty Leadership Development, LLC
1 – Unique ID remains the same for recurrent meeting.
  • Change the password every month.

2 – Please **do not post** WebEx Teleconference information such as links to meetings and password for access on websites (including vTools Meetings registrations).
  • Email it **directly** to your members (e.g., via eNotice/Listserv mailing list).
  • Attendees should only get the link through eNotice if they register in vTools.
3 – The **host** should have a [WebEx](#) account to open the meeting and let people in.

4 – Make sure, as a host, to grant “**presenter**” status to whom it will present content and they share their presentation only.
WebEx – How to use / Lessons Learned

Membership Development - Training Topic

5 – WebEx does not replace vTools.
• Use vTools and eNotice to send the WebEx link to the meeting registrants.
• eNotice needs to be sent “Express” at a minimum 3 hours before meeting start with no attachments.
WebEx – How to use / Lessons Learned

Membership Development - Training Topic

6 – There are 2 places where you can lock the meeting.

If the host is **not** a presenter.

If the host is a presenter.
WebEx – How to use / Lessons Learned

Membership Development - Training Topic

7 – You can just mute participants or “Expel” them from the meeting.
THANK YOU