Dear League Leaders:

Many of you have or will have candidate forums using Zoom in the coming weeks. A recent candidate forum in New Hampshire was “Zoom Bombed” (https://www.conwaydailysun.com/news/local/internet-trolls-zoom-bomb-league-candidate-forum/article_0742150a-088e-11eb-b536-efeb7db116e0.html) and had to be aborted. Given that, we are offering some advice on how to avoid Zoom Bombing.

By controlling the Zoom format and the Zoom settings, you can minimize or eliminate the chance of Zoom Bombing.

**Use Zoom Webinar**

Zoom has two formats that can be used for candidate events: Zoom Meeting and Zoom Webinar. Most of us have experienced both: a Zoom Meeting has one type participant who joins with a meeting link and, in general, can appear on screen, and can speak.

Zoom Webinar has two types of participants: panelists, who can speak and be seen; and attendees, who can neither be seen nor heard (unless invited by the host), but can watch the forum and submit questions live. Panelists are invited to the webinar by the host, and receive an email via Zoom with a unique link to join the forum. Attendees usually join by registering in advance, getting a unique link in an email via Zoom, and joining the forum when the host starts it.

If you use Zoom Webinar it is extremely unlikely that the forum will be Zoom Bombed, because you control who are the panelists. The potential bombers, the attendees, cannot show video, speak, or share their screen. So, only people you know; the candidates, moderator, host, and other forum “staff” would be able to disrupt the forum.

Zoom Webinar is available from the LWVMA shared webinar account (contact bgorman@lwvma.org), or Leagues can purchase the webinar add-on to a Zoom Meeting account for $40/mo. Zoom Bombing will not happen during a webinar because only panelists have audio, video and sharing privileges, and even these can be curtailed.

**Use Zoom Meeting Carefully**

Zoom Bombing is most disruptive when the forum uses Zoom Meeting (rather than Zoom Webinar). Unfortunately, this eliminates the possibility of allowing the general public to join and ask questions.

Generally Zoom Bombers infiltrate your Zoom Meeting by either finding the join link posted on the internet or obtaining the link through a registration process. The bombers join the meeting and bombard the audio and video with unwanted content.

The first line of defense against a bombing is controlling who joins your Meeting. Here are some suggested measures:
• Never post the link to join a Zoom meeting in a public setting.
• Only give the link to join to people you know.
• Use a passcode.
• Require registration to join the Meeting.
• Enable the Waiting Room so participants cannot join until host admits them.

The details on how to execute these settings can be found on the Zoom support website. 
https://blog.zoom.us/keep-uninvited-guests-out-of-your-zoom-event/

**Showing the Forum Live with Zoom Meeting**

If you want to be absolutely sure the public will not see your forum get bombed, do not show it directly from Zoom in any live format (Facebook/YouTube Live). Note: Showing live using Zoom Webinar is safe from Zoom Bombing.

You can post your own Zoom recording or you can work with your local cable station so they can record the forum and post it soon afterward. If you are recording, explain your plan to the candidates, and assure them that the forum will be shown in its entirety and will not be edited except to correct technical glitches.

But, *if you are careful* about admitting only those known to you, you can successfully use Facebook/YouTube Live or broadcast the forum live in collaboration with your local cable station. We advise that you also record the Zoom session as a backup.

Although Zoom was not developed for candidate forums, in this pandemic it has become a safe alternative to live forums. We should not let the fear of Zoom Bombing prevent us from carrying out our critical role of hosting non-partisan candidate forums.

Written by Karen Price
10/12/2020