Beware of Zoombombing

According to a New York Times article, there's a new type of malicious behavior proliferating called Zoombombing. This is when people find publicly posted links to Zoom meetings, crash the meeting and then share their screen to display pornography or other inappropriate materials.

Be aware that if you post a Zoom link publicly, such as on a website or on social media, this opens you up to this type of behavior. You can avoid this by:

- Only emailing the link out to people in your congregation;

- Requiring a password for your meeting, and emailing it to people who ask.

This, of course, makes it more difficult to be the welcoming presence you probably wish to be. If you still want to publicize your Zoom link publicly, there are some precautions you can take:

- Familiarize yourself with the "Manage Participants" controls. As the host of a meeting, you can stop someone else's screen share. You can also remove someone from a meeting. **Read Zoom's guide here.**

- Only allow meeting hosts and co-hosts to share their screens. This can be done universally for all of your meetings via the "settings" section of your account. Or, when you start a meeting you can access the **Screen Share** controls (click **^** next to the **Share Screen button**) and can choose to only allow the host to share his or her screen. **Find Zoom's information on this here**.

  If more than one person needs to share their screens during the service or meeting, you can make the other presenters "co-hosts."

[Find Zoom's co-host information here](#).

[Find our Quick Guide to Zoom here](#).

Author

[Tiffany Vail](#)

Tiffany Vail is the Associate Conference Minister for Communications for the Southern New England Conference of the United Church of Christ.