Stopping Zoombombing Trolls ~ A Short Tutorial

V 4/1/2020

What is Zoombombing?

Think of Zoombombing as a virtual 'party crasher'. It's when uninvited people access your Zoom meeting and display offensive, cultural inappropriate or pornographic content. It's been an increasing problem, and Zoom is working hard to address the issue.

What can I do to prevent this?

Be educated! The internet has a wealth of information about this. Some is better than others. Two particularly good articles are from the NY Times and the Anti-Defamation League (links below). YouTube has a series of videos, too, with step-by-step instructions.

https://www.nytimes.com/2020/03/20/style/zoombombing-zoom-trolling.html

https://www.adl.org/blog/how-to-prevent-zoombombing

Where should I start?

Be proactive:

- Do NOT post a zoom link to social media; posting to a public forum invites trouble.
- Do NOT allow invited guests to share their invitation. If an additional invitation is required, the host of the meeting should be contacted for further instructions.
- Require a password for the meeting and include it in the email invitation.
- Learn which Zoom settings can help thwart an attack.
- Decide before the meeting what will happen if all your efforts fail and the party crashers keep appearing and inform the meeting attendees what the plan is, so they are not surprised.

What will change if I use a Diocesan Zoom Account?

- Canon Barbara Martin will manage all the settings from the administrative end of our account. Don't worry, we'll do this slowly and in stepwise fashion. If you host a meeting that gets Z-bombed, please follow your meeting plan, and then contact her as soon as possible at 207-650-6070.
- Some of those settings can be changed while your meeting is in progress. If you decide to change the settings, please be aware that your meeting will be more vulnerable.
- The person who arranges the meeting should be the 'host' and should log into the Zoom account and start the meeting from there. ***After the meeting, the host needs to sign out of the account (upper right-hand corner; left click on the diocesan logo to see the words 'sign out', click).***
- Everyone else (guests) should access the meeting from the link provided. Only the host should be logged into the Zoom account.

In addition to the information in the "Be Proactive" section above, what should I be considering if I host a meeting from the Diocesan account, have my own account, or manage my congregation's account?

- ➢ For non-Diocesan accounts: Before your meeting starts, go to your account and click on "Settings" in the left-hand menu, Scroll down to "Screen sharing" and under "Who can share?" click "Host Only", and then click on "Save"
- ➢ For all: Be familiar with the "Manage Participants" controls. As host, you can stop some else's screen share and remove them from a meeting by using the "Manage Participants" tool and click "Pop Out" to see the participants list. Hover over a participant and click more for a list of actions. "Remove" is the last one on the list. Once removed, a person cannot rejoin the meeting.

Any other hints?

- ➢ As an administrator of your own/congo account, you can do the following (many of these functions are accessed using the 'Settings' tab on your account dashboard so the changes are effective for everyone who is sharing the account):
    - ✓ Require participants to register for your meeting
    - ✓ Change screensharing setting to "Host Only"
    - ✓ Disable "Join meeting before Host" so the bad guys can't start trouble
    - ✓ Enable the waiting room
    - ✓ Require a password
    - ✓ Disable participant sharing and file transfer so there's no digital virus sharing capability
    - ✓ Turn off person to person chat
    - ✓ Start meeting with participant video off
    - ✓ Instruct participants NOT to share the link
    - ✓ Remove disruptive participants
    - ✓ Disable 'allow removed participants to rejoin" so booted attendees can't slip right back (although they may change their identity and try again anyway)
    - ✓ Remember to tell your guests what will happen if your meeting is crashed so they're not surprised.

Help! I'm stuck and don't know what to do!

Take a deep breath and try again. Try YouTube for a step-by-step visual tutorial. Reach out to Canon Martin at bmartin@episcopalmaine.org or 207-650-6070 if you have a specific question or need support.

We can take steps to make it harder for crashers to access our Zoom accounts, but that also makes us a challenge, and more will try, but we can work together to keep our Zoom community safe ~ thank you for your help!

Zoom Guidelines for Diocesan Accounts (draft 4/1/2020)

Two Zoom hosts are maintained for diocesan use
zoom@episcopalmaine.org and zoomtwo@episcopalmaine.org

DO: remember that only one meeting per account is possible, and scheduling is on a 'first come, first served' basis.
DON'T: schedule over someone else.

DO: be familiar with the zoom addresses (above) and passwords.
DON'T: repeatedly try to log in. Doing so will trigger the account security and lock everyone out for at least 30 minutes.

DO: feel free to use either zoom or zoomtwo
DO: indicate in the title who is the host. Example: Diocesan Staff Meeting (Barb), so if there's a problem, Canon Martin knows who to be in touch with.
DO: use the pre-arranged settings. Changing them may make your meeting more vulnerable to Zoombombing. Please be in touch if you have questions about the settings.
DO: log into the Zoom account if you are the host.
DON'T: log into Zoom if you are not the host ~ please use the link provided in your invitation.

DO: check when you start a meeting to make sure there's no other meeting currently in progress. If you start your meeting before they're done, you will prematurely end their session.
DO: start and end your meeting on time.

DO: Test your mic and speakers before the meeting starts by opening the menu (upward caret) next to the mic icon in the lower left-hand corner of the Zoom screen.
DO: Check the orientation of your camera. Can others see your entire face? Is there a plant growing out of the top of your head? Is there glare from a light or window?

DO: Ask everyone who is not speaking to mute their mics. This avoids feedback and echoing. Guests can mute themselves, or the host can mute from the host control toolbar.

DON'T: hesitate to be in touch if you have questions or concerns!

.