KEEPING SAFE ON ZOOM

KEEPING UNWANTED GUESTS OUT

LIMITLESS

31st MARCH 2020

Contents

INTRODUCTION

As we've all been forced into isolation to keep the county and world safe, the growing trend to find online solutions to keep in touch with church congregations, families and friends along with creating online consortiums to help each other tackle the new challenges, a new phenomenon has been arising. ZOOM BOMBING.

Zoom Bombing is the latest issue arising when you don't have relevant security settings in place to open up your meeting to people you don't know. Unwelcome guests join your meetings and share their screens which quite often contain racist or pornographic material and open their microphones and speak racist remarks over the presenter.

Quite often in zoom, the settings are set for meetings where you know who you're inviting and there's very little risk of intruders. But what happens when you share a meeting link on Facebook or on your website? Well, anyone can join and they can also create havoc.

Here are some steps to help reduce the likelihood of an unwanted guest in your meeting and also limit the amount of power an intruder has to disrupt your event.

SETTING UP YOUR ZOOM ACCOUNT

All of these settings are in settings in your web portal for zoom. We suggest you adjust these ones accordingly **BEFORE** scheduling a zoom meeting.

1. **Always Use a Meeting Password.** This can be turned on as standard. This stops people guessing your meeting code and just joining the meeting by chance or brute force.
   Settings > Meeting > Require a password when scheduling new meetings = ON
   a. You may also want to include embedding your meeting password in the link if you're emailing the link to people.
   Settings > Meeting > Embed password in meeting link for one-click join = ON
2. **Mute Participants Upon Entry.** This may seem mean and counterintuitive. However, if they're muted on entry, it stops them instantly shouting out unwanted words but also feedback.
   Settings > Meeting > Mute participants upon entry = ON
3. **Turn Private Chat Off.** This stops 1:1 chat. This eliminates offensive chat which you, as the host, cannot see.
   Settings > Meeting > Private chat = OFF
4. **Turn Off File Transfer.** This disables the possibility of people sharing files through the chat function. Unwanted files can often contain pornography or computer malware which can then be used to hack people's computers and share personal information.
   Settings > Meeting > File Transfer = OFF
5. **Turn Co-Host On.** This allows you to nominate another participant (once in the meeting) to help you manage the other participants and co-host the meeting.
   Settings > Meeting > Co-Host = ON
6. **Allow Only The Host To Share Their Screen.** This is **ESSENTIAL**. Allowing participants to share their screen will cause havoc. Hosts and Co-hosts can share their screens when this option is enabled.
   Settings > Meeting > Screen sharing = ON

Further options in this section should then be greyed out.

7. **Disable Desktop/Screen Share For Users.** This option only lets you share an application window rather than your whole desktop. This one isn't essential, however, it does save some embarrassment or other people seeing your email whilst you're switching through applications.

Settings > Meeting > Disable desktop/screen share for users = ON

8. **Turn Annotation OFF.** This again is **ESSENTIAL.** Annotation allows users to add information to shared screens allowing them to draw or write over your presentations. This can be distracting and disturbing.

Settings > Meeting > Annotation = OFF

9. **Turn Whiteboard OFF.** The whiteboard is a feature that allows users to draw something or write something and share it with the rest of the participants. Again, zoom bombers use this to draw or write offensive content.

Settings > Meeting > Whiteboard = OFF

10. **Turn Allow Removed Participants To Re-join OFF.** This again is **ESSENTIAL.** If you block a participant during a meeting (click on the more button in the participants panel against their username and select Block user) unless this is selected, they can re-join instantly.

Settings > Meeting > Allow Removed Participants to Re-join = OFF

11. **Turn Waiting Room ON.** This feature is also **ESSENTIAL** to tackling unwanted visitors. It also give you access to the meeting before the guests. When people join they are put in a waiting room until you let them in. You can either admit them one by one (very useful if you want some people to co-host as you can admit them first, elevate their control and then admit others) or all at the same time. This delay also allows you to edit in meeting settings like disabling "allow participants to unmute themselves" or "participants can chat to everyone" depending on your preference.

The other settings under this section are up to you as to how your account and organisation is set up.

Lastly, you can set a title, logo and description for your waiting room holding screen.

Settings > Meeting > Meeting(Advanced) > Waiting Room = ON

All other options are optional. BEWARE as enabling some other options may disable some of your preferred settings.

SCHEDULING A MEETING

Here are some options to look out for when scheduling a meeting

1. **Request Registration**. If you're opening up your meeting to people you don't know personally, this is a great function to deter unwanted intruders.
   When you enable this function, participants have to log on (via a link you can email out) and give you their information before receiving the meeting link. There's lots of options with this. Check out https://support.zoom.us/hc/en-us/articles/211579443-Registration-for-Meetings for more info.
   Meeting > Schedule a meeting > Registration
   a. When setting up registration enabled meeting there is an option to share the registration link on social channels. This is on as standard. Ensure you de-select this to keep your meeting as safe as possible. These are found at the bottom of the meeting page.
      *My Meetings > Manage "**meeting name**" > Registration > Registration Options > Edit > Show social share buttons on registration page = OFF*

2. **Meeting ID.** Select "generate automatically". This creates a random code for your meeting. **DON'T** use your personal meeting ID.
   Meeting > Schedule a meeting > Meeting ID = Generate Automatically

3. **Meeting Password.** This should be on as standard. But double check it. A box should appear with a code in. This is your meeting password.
   Meeting > Schedule a meeting > Meeting Password = ON

4. **Meeting Options.** There a few settings here.
   a. **Enable Join Before Host:** This allows people to join the meeting before you. If you have a waiting room then they will be sent to the waiting room. If not, they will enter the meeting and can cause havoc even before you get there to moderate. We would suggest having this OFF as standard. They participant will see a screen saying the host hasn't joined yet.
      Meeting > Schedule a meeting > Meeting Options > Enable Join Before Host = OFF
   b. **Mute Participants Upon Entry.** We would suggest having this enabled. It means everyone's microphone is muted when they join the room. It help with unwanted chatter and feedback.
      Meeting > Schedule a meeting > Meeting Options > Mute Participants Upon Entry = ON
   c. **Enable Waiting Room.** This should be on as standard if you have enabled it in your settings. Just double check.
      Meeting > Schedule a meeting > Meeting Options > Enable Waiting Room = ON

Hit Save.

You will now see an overview of all your settings for the meeting. Copy the invitation link, or registration link and send to your participants.

DO NOT SHARE YOUR MEETING LINK TO SOCIAL MEDIA UNLESS YOU ARE MANUALLY REGISTERING PARTICIPANTS

MEETING CONTROLS

BEFORE THE MEETING STARTS:

If you've used all the relevant settings above, you should now be ready to start your meeting. Go on, Have a go!

In the meeting you should be the only person in there (unless you've changed a few settings to allow others to bypass the waiting room).

Here's the settings to look for next to ensure a safe meeting.

1. **Turn Allow Users to Un-mute Themselves OFF.** This is **ESSENTIAL**. This, as it eludes too, stops users being able to activate their microphone. The meeting host or co-host can activate their microphone in the participant's panel. Also using the "raise hand" feature helps identify when people want to speak.
   Manage Participants > More > Allow Users to Un-mute Themselves = OFF

2. **Activate Only Chat With Host.** This does as it says. Only allows participants to chat with the host rather than broadcasting messages to ALL the participants. Zoom Bombers use this to send offensive and upsetting messages to everyone and also individuals privately. Enabling this feature allows them only to send messages to you. Whilst this is entirely up to you, we would recommend it.
   This feature can also be changed whilst the meeting is happening. So if you're happy that everyone in the meeting is supposed to be there, then re-activate the chat feature for everyone!
   Chat > More (3 dots) > Participant Can Chat With > Host Only = ON

3. **Check Only Host Can Share Screen.** This should be on already. But its' worth checking!
   Share Screen > More (up arrow next to green share screen symbol) > Advanced Sharing Options > Who Can Share? > Only Host = ON

ADMITTING CO-HOSTS

You're now ready to admit your co-hosts. These are the people you trust and want to allow to help you run the meeting. They may also be presenters as well as other moderators.

1. **Admit Your Trusted Moderators & Presenters.** Click on Manage participants and you will see a list of people waiting and a list of people in the room. To admit someone simply hover over their name and select "ADMIT"
   *Manage Participants > Waiting > **Participant Name** > Admit*

2. **Elevate To Co-Hosts.** This allows your trusted helpers to help moderate the event and also co-presenters to unmute their own microphone and share their screen. Hover over the participant name, select more and select "Make Co-Host"
   *Manage Participants > In Meeting > **Participant Name** > More > Make Co-Host*

You're now ready to admit your participants!

IN THE MEETING

1. **Admit Your Participants.** You can add them one by one or all at the same time. The same way as you did your co-hosts. Just don't elevate their permissions!
   Manage Participants > Waiting > **Participant Name** > Admit
   OR
   Manage Participants > Waiting > Admit All

2. **Block Any Unwelcome Guests.** Yes, you may still get some unwanted guests. The best way to find out if they're supposed to be there is to chat privately to them. Quite often they send you back an expletive or something that you really wouldn't expect. This gives the game away that they're not supposed to be there whilst not interrupting the meeting.
   a. **To Chat Privately.** *Chat > To: > **suspect participant name***
   b. **To Block a Participant.** *Manage Participants > **Participant name** > More > Remove*

3. **Using Raise Hand.** Guests can show an express to want to talk or give a comment by using the raise hand function. This is found in the participant's panel. This displays a hand next to the participant's name that wants to speak.
   If someone else raises their hand they are moved to the top of the list under the last person to raise their hand.
   Participants > Raise Hand

4. **Un-muting and Muting Participants Microphones.** Whilst doing this remotely is a little tiresome, it does mean that only the people you're asking to speak can speak.
   In the participant's panel, find the participant you want to un-mute, hover over their name and select "un-mute". This then sends a message to the participant informing them that the host wants to un-mute their mic and asks if they want to stay muted or un-mute. **WARNING** if they don't un-mute, they can later unmute themselves with no warning. So be careful who you give permission too.
   To re-mute them, hover over the participant name and select MUTE.
   a. **To Unmute -** *Manage Participants > **Participant Name** > Un-Mute*
   b. **To Mute -** *Manage Participants > **Participant Name** > Mute*

5. **Lock The Meeting.** Once you've got everyone you're expecting into the meeting you can lock it. Doing this prevents anyone else from joining the meeting. They can't even gain entry to the meeting room. This is really useful when you're running small groups via zoom as you know who's supposed to be there!
   Manage Participants > More > Lock Meeting

BREAK OUT ROOMS

This, whilst being one of Zoom's most favourable features for churches and youth groups, is also one of its least secure.

When guests are in the breakout rooms, they all have control over their own microphone and they can all share their own screens.

So, as a warning, be wary of using breakout rooms in an "open" meeting.

For further information on how to use breakout rooms, go to: https://support.zoom.us/hc/en-us/articles/206476093-Getting-Started-with-Breakout-Rooms

USEFUL LINKS:

Here are some useful Links to help you with your journey to becoming a Zoom Pro:

Zoom: https://zoom.us

Zoom Support pages: https://support.zoom.us

Zoom Blog: https://blog.zoom.us

Zoom Privacy Policy: https://zoom.us/privacy

Techcrunch.com Blog Post on Zoom Bombing: https://techcrunch.com/2020/03/17/zoombombing/