Zoom Policies

1. What We Aim to Prevent

The Federal Bureau of Investigation recommends exercising due diligence and caution in organizational cybersecurity efforts due to a recently increased risk of video-teleconference hijacking, colloquially known as “Zoom-bombing”. The goals, steps, and information outlined below are being recommended to ensure the safety and security of all Zoom meeting attendees by mitigating the risk of teleconference hijacking threats.

We aim to prevent (a) unknown, unapproved, or otherwise unwelcomed persons from (b) gaining access to a First UU hosted, led, or sponsored online meeting or gathering, in order to further prevent (c) the exposure of any welcomed meeting-attending member or guest to offensive, harmful, lewd, or otherwise inappropriate material, including but not limited to pornography, gore, violent imagery, slurs, hate speech, irrelevant sexual content, threats, and more.

In plain speech, the goal of these requirements and suggestions is to prevent any malicious outside actors from gaining access to one of our online meetings to share harmful, inappropriate, or disruptive content. As defined above, the act of doing so has become colloquially known as “Zoombombing”. The good news is that the risk of having one of our meetings “bombed” by an outside actor should drop significantly (almost to 0, though reasonable caution should always still be exercised) if a selection of settings and practices are enacted by all of our licensed hosts. These settings and practices are further outlined below.

2. Required and Suggested Settings

The following account settings should be enabled or disabled as described. Explanations follow.

Under "Schedule Meeting"

1. Participants Video – OFF
2. Use Personal Meeting ID (PMI) when scheduling a meeting – OFF
3. Require a password when scheduling new meetings - ON
4. Require a password for instant meetings - ON
5. Require a password for Personal Meeting ID (PMI) - ON
6. Embed password in meeting link for one-click join – ON
7. Mute participants upon entry – ON

Under "In Meeting – Basic"

8. Play sound when participants join or leave – ON
9. File Transfer – OFF
10. Co-Host – ON
11. Screen Sharing – ON, HOST ONLY
12. Disable desktop/screen share for users - ON
13. Annotation – OFF
14. Whiteboard – OFF
15. Remote Control – OFF
16. Allow Removed Participants to Rejoin – OFF

Under "In Meeting – Advanced"

17. Remote Support – OFF
18. Far End Camera Control – OFF
19. Virtual Background – OFF
20. Identify guest participants in the meeting/webinar - ON
21. Waiting Room – ON, ALL PARTICIPANTS

Under "TELEPHONE" near top of screen

22. Mask phone number in the participant list – ON

Under "RECORDING" near top of screen

23. Local Recording – OFF
24. Cloud Recording – OFF
25. Automatic Recording – OFF
26. Recording Disclaimer – ON, "Ask Participants for consent"

Details

1. Participants Video – OFF

Turning off participant video simply requires each participant to manually enable their video feed after joining the meeting. It is good Zoom etiquette, and it allows an extra layer of security or an extra moment to react to an unexpected presence.

2. Use Personal Meeting ID (PMI) when scheduling a meeting – OFF

Think of your PMI as your home address – you trust some people with the information, but wouldn't want to share it with everyone. Anyone who has your PMI can use it to drop in to knock at your door at any time. It's best to schedule meetings with a unique one-time meeting ID instead of your PMI. Reserve your PMI for other uses.

3. Require a password when scheduling new meetings – ON

This is a necessary layer of security. If you enable #6 below, it also adds almost no additional burden for the protection it provides. Without this password in some form or fashion, Zoom users will not be able to gain access to your meetings.

4. Require a password for instant meetings – ON

See #3 and #6 for more information.

5. Require a password for Personal Meeting ID (PMI) – ON

See #2, #3, and #6 for more information.

6. Embed password in meeting link for one-click join – ON

This is a fantastic tool that allows you to take full advantage of password protection without inconveniencing participants. With this setting enabled, the password needed to access the meeting is embedded in the link in your copy-and-paste invitation. No one will need to type anything in – the computers will do that work for you.

7. Mute participants upon entry – ON

For the same reason as #1, mute participants' microphones upon entry and leave it to them to manually unmute themselves.

8. Play sound when participants join or leave – ON

This is a useful tool for the host and will be discussed more in #21. This essentially acts as a bell above the door to your Zoom "room". When anyone enters or leaves, either the host or the host and all participants (your choice) will hear a chime sound. This allows you to monitor who is coming and going.

9. File Transfer – OFF

Arrange for files to be transferred outside of Zoom, perhaps via email, if necessary. Turning this setting off closes off another avenue for bad actors to drop materials into the meeting.

10. Co-Host – ON

Enabling and naming a co-host provides a backup layer of both security and function. It is similar to having a co-pilot – an extra pair of hands in case something comes up. It also means that should the original host need to leave the meeting for whatever reason, it can continue without them through the co-host. All meetings of more than 5 to 6 people should have a host and a co-host assigned. Meetings of 5-6 or fewer may make this decision for themselves.

Each group should designate a "tech host" in addition to the primary host; this may be the co-host or it may be another group member, and their role will be to support the meeting through managing the waiting room, monitoring audio muting/unmuting and video feeds, and other such virtual room management needs through Zoom.

11. Screen Sharing – ON, HOST ONLY*

Screen sharing is a useful tool and needn't be disabled entirely. With account settings set to "Host Only", participants won't be able to share their screen in your meetings by default. If needed, you can temporarily change this setting within the meeting, which will allow others to request to share and you to approve or deny their request. If your group regularly utilizes screen sharing as a meeting tool, you may instead set this option to ALL PARTICIPANTS. Think critically about your audience and your group's needs when you make this selection. Also, see #12.

12. Disable desktop/screen share for users - ON

This is an extension of #11, but there are some group dynamics wherein a host or group may wish to have this setting turned OFF to allow users to share their screen with the group.

13. Annotation – OFF

Annotation allows participants to draw, doodle, and type on the image of a shared screen. See #14.

14. Whiteboard – OFF

This is a shared collaborative doodle and writing space for the meeting, similar to the Annotation function but without need for a shared screen canvas. Disabling these two settings is akin to hiding the chalk and markers when the teacher isn't using them so that no one gets carried away.

15. Remote Control – OFF

Remote Control allows participants to request access to interact with the contents of a shared screen. It is similar to the idea of remote desktop operation software. It can allow for great collaboration, but is also a mighty risk if you aren't 100% sure of your co-participants. See #17 as well.

16. Allow Removed Participants to Rejoin – OFF

There is no reason to enable this setting. Ensure it is turned off. Turning this setting to OFF is like installing a lock on your front door – if you kick someone out, they're not getting back in.

17. Remote Support – OFF

This is similar to #15. It allows a participant to take remote control of your computer through Zoom. This is not recommended unless one-on-one with individuals you trust and know well.

18. Far End Camera Control – OFF

Enabling this setting would allow a participant to request access to your camera or webcam. This is a security risk. Ensure this setting is turned off.

19. Virtual Background – OFF

Whenever possible, disable this setting. It provides another avenue for people to share unapproved images. If virtual backgrounds are necessary for participant privacy, discuss on an individual basis.

20. Identify guest participants in the meeting/webinar

This allows the host to see who is a user associated with the host account and who is not. It's simply an added layer of information for the host to use at their discretion.

21. Waiting Room – ON, ALL PARTICIPANTS

This setting is crucial to enable. The waiting room is exactly what it sounds like – a virtual antechamber that participants enter before the meeting – and allows the host to admit people into the meeting manually (one by one), or to admit all waiters into the meeting room upon reviewing the list. If someone enters a meeting late, they will still be placed in the waiting room until they're approved to enter the meeting. Having "play sound when participants enter or leave" will help hosts keep track of anyone waiting to be admitted, as will a visual notification at the bottom of the screen.

Under "TELEPHONE" near top of screen

22. Mask phone number in the participant list – ON

If a participant calls in via phone instead of using their computer, their phone number will show in place of their name. For reasons of safety and privacy, masking their number prevents other participants from seeing the entire number. For example, it may show 28******22 or 83******14.

Under "RECORDING" near top of screen

23. Local Recording – OFF

Disabling this setting prevents hosts and participants from recording the meeting via Zoom and saving the recording to a local file on their machine.

24. Cloud Recording – OFF

Disabling this setting prevents hosts and participants from recording the meeting via Zoom and saving the recording to their Zoom account via the Cloud.

25. Automatic Recording – OFF

Disabling this setting prevents your meetings from being automatically recorded and saved. Always enable or disable screen recording on an as-needed basis; don't rely on automatic recording.

26. Recording Disclaimer – ON, "Ask Participants for consent"

If you plan to record meetings or think that you might one day, please enable this setting. This will show a popup message to each participant allowing them to either continue with the meeting knowing that it is being recorded or to leave the meeting should they not consent to being recorded. Never record a meeting without the explicit permission (consent) of each participant in said meeting.

3. Good Digital-Interpersonal Practices

1. Guard Meeting Links and Passwords – Loose Lips Sink Ships

Best practice is not to share password-embedded meeting links or meeting passwords *without permission*. Links to Zoom meeting should be shared in the all-church Newsletter or TUUCAnnounce only, with social media posts used as a gatekeeping advertisement and invitation to request access to a given meeting or group. Meeting links may not be posted publicly. If meetings are open to children and families, use extra caution in disseminating links to others.

2. Lock Down Your Own Account Settings First

By securing your own global account settings, you set yourself up for greater success in creating a secure meeting than you would in trying to create a secure meeting starting with a less-secured account. A secured account – with some combination of the required and suggested settings – creates a good foundation to build upon.

3. Use Strong Account Passwords

While this has not appeared to be a major issue yet, it is always good practice to have a secure password to protect your own account. This is especially important for Host accounts through the First UU Business account, particularly those with shared scheduling permissions.

Other Security Concerns

There are some relatively minor yet not insignificant concerns with security that don't just boil down to bombing. Zoom admittedly does not have a stellar track record when it comes to honest transparency about their systems - a few weeks ago, it came out that they were not actually utilizing the end-to-end encryption for each meeting that they advertise as a system feature. There was also a feature up until a few days ago that allowed for data mining through LinkedIn and to Facebook without needing the knowledge or consent of any participants. Finally, there were security issues last year specifically with Macintosh operating systems that essentially left a backdoor cracked for bad actors to gain control of live webcams without the knowledge or consent of the user. They've since patched that issue, but it all adds up to a bit of a suspicious track record.

Concerned individuals might create an entirely new email address to use for their Zoom account, use an incognito web browser window to operate zoom.us, lock down their other accounts and passwords according to best security practices, keep their Zoom software up-to-date, manually obstruct their webcam when not in use, and/or call in via phone (without using a computer at all) to avoid signing in or creating an account (though this will limit usability).