ZOOM BOMBINGS
PART 1

What They Are and How to Avoid Them

An overview of Zoom security tips and features when hosting a meeting

BSSI
Where Peace of Mind is Found
Simplified IT Support / Solid Security / Sound Relationships

740.475.1700
ask@BSSI.biz
www.BSSI.biz

TABLE OF CONTENTS

INTRODUCTION

Zoom, a video conference application, has become a heavily used communication tool as people across the world are being told to stay at home to prevent the spread of the coronavirus. USA Today reported, during March 2020, daily downloads of Zoom in the U.S. rose more than 1,000% from 29,802 to 339,701, outpacing social media apps Facebook, Snapchat, and TikTok.

Unfortunately, with the increased activity, Zoom has become one of many targeted applications as hackers seek to take advantage of people migrating to virtual environments due to the coronavirus. The media has reported on a recent security concern called "Zoom bombings" (aka hijackings) – earning its name from uninvited guests joining a zoom videoconference and sharing their screen with real attendees to display disturbing pornographic, hate images, racist content and threatening language.

While several other Zoom data privacy and security concerns are being discussed in the media, there are some issues, such as Zoom-bombing, that are not due to technological weaknesses in the application. Rather, there is security readily available for us to utilize when hosting a Zoom meeting to help prevent being a victim of Zoom-bombing.

The best way to maximize Zoom security is to prepare for a meeting in advance and follow some simple tips from two perspectives: (1) Host setup of the meeting (2) Host control of the meeting.

In part one of this series we will be covering general use of Zoom and security tips and features that can be used when a Host sets up a meeting.

Before we jump in, there are a few things to note:

1. If you are familiar with Zoom and want to skip directly to the security tips go to the second section of this post titled "Zoom Security Tips".

2. The Zoom desktop applications (PC or macOS) and the mobile applications (Android or iOS) are similar but do have minor differences. The print screens in this article are from the Zoom Basic (Free) application using a PC Desktop.

3. The desktop application does provide the capability to schedule zoom meetings with basic security options. Logging into your zoom account on the web portal provides advanced host security setting options.

4. The host security features available depend upon the zoom version which varies from Basic (free) to Standard Pro to Telehealth.

How to Use Zoom as a Meeting Host

If you want to host a zoom meeting, you must have a zoom account. (To sign up for a zoom account go to https://zoom.us/signup.) This will allow you to create instant and scheduled meetings and send invitations to attendees. Your account, hosted on Zoom's web portal, is from where you can access your personal settings, update your profile or upgrade your plan at any time.

Zoom offers a free version account that limits the meeting length to 40 minutes and a Standard Pro version for a monthly fee of $15 with unlimited length meetings. (They also offer other versions including Telehealth).

When a Zoom account is created, you are assigned a Personal Meeting ID (PMI). This numeric code is your default meeting ID to share with attendees when creating a meeting. It does not expire and can be used repeatedly.

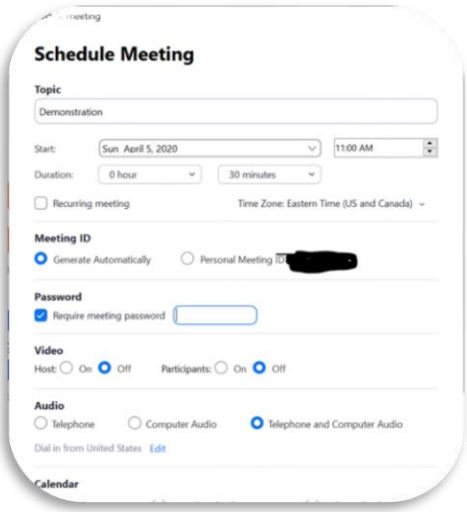
Zoom offers two ways for the host to schedule a meeting:

1. Schedule from the Zoom desktop client or mobile app
2. Schedule from the Zoom web portal

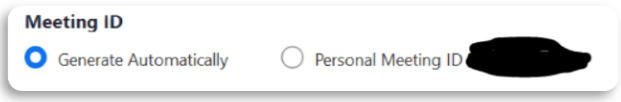
The below information is from the desktop perspective.

Scheduling a Meeting with Zoom

When opening the "schedule a meeting" option, a screen like the below is displayed.

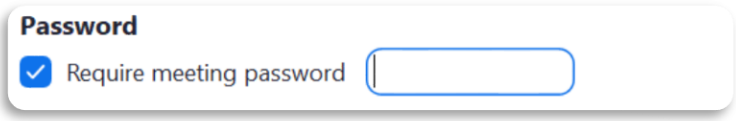


A. Meeting ID



You can use your default personal meeting ID (PMI) that was originally assigned to you when you created the Zoom account or generate a unique meeting ID for this specific meeting. As a general rule of thumb, if the meeting has a high number of attendees or includes strangers select "Generate Automatically" under the ID options. For regularly scheduled meetings with your team, family, or friends it is typically more convenient to use your PMI so you don't need to generate and communicate a new meeting code for every recurring meeting.

B. Password



You have the option to require a meeting password. This is an excellent security layer.

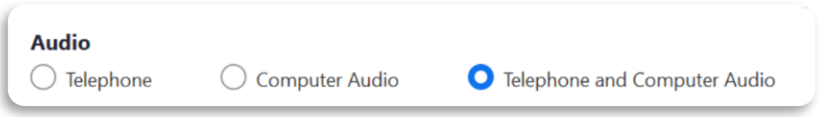
C. Video

Host: Choose if you would like the host video on or off when joining the meeting. Even if you choose off, the host will have the option to start their video. Default to off.

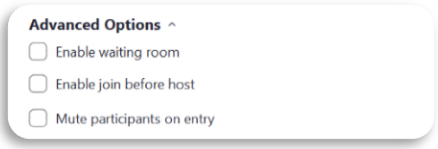
Participant: Choose if you would like the participants' videos on or off when joining the meeting. Even if you turn off, the participants will have the option to start their video. Default to off.

D. Audio

This determines how you will allow attendees to listen to the zoom meeting. (Please note Zoom added telephone dial-in numbers in 03/2020 to address the current high demand. You will see the expanded list of available dial-in numbers when you join a meeting. So, when joining a Zoom meeting and using the phone audio option, you receive a busy signal, hang up and try one of the other numbers.)



E. Advanced Options on the Schedule Screen



A zoom meeting can start in one of 3 ways depending upon the Advanced option selected.

1. Enable waiting room

   This option mandates that the meeting can only start when the host says it can start. The Waiting Room feature also allows the host to control who and when an attendee joins the meeting. When the attendee joins a meeting with "Waiting Room" enabled, they will see a message similar to "Please wait, the meeting host will let in join soon". This message can be customized by the Host.

   The attendee stays in the waiting room until the host lets them in which the Host can allow all in at one time or select attendees one at a time to join.

2. Enable join before host

   This option allows attendees to join the meeting before the host is on the meeting. The meeting can also be held without the host altogether in case the meeting is run by someone else on behalf of the host.

3. If options 1 or 2 are not selected by the Host

   When the attendee logs into a Zoom meeting they will see the following message "The meeting is waiting for the host to join". However, the attendees can begin talking with each other the moment the attendees log into the meeting regardless if host has the started the meeting or not. To prevent this, you can select "Mute participants on entry".

   For small groups of people who know each other, it's common for people to join the meeting and make small talk while waiting for the host and other attendees to join. In that case, your Host would not check any of the above 3 advance options.

How to Use Zoom as an Attendee

A Zoom account is not required if you are joining a Zoom meeting as an attendee. If someone invites you to their meeting, you can join as an attendee without creating an account.

However, you must have the Zoom application installed on the device (desktop, smart device) from which you plan to join the Zoom meeting. Zoom software is available for download for PC and macOS desktops and Android and iOS smart devices. You do not need to create an account to download the application.

Note: Only use these sources for downloads: Desktops - zoom.us/download and Google Play and the Apple App store for smart devices.

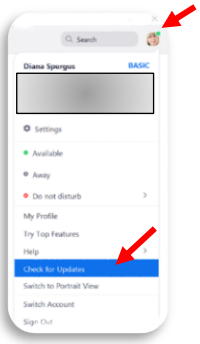
Zoom Security Tips

Security Tips for Hosts and Attendees

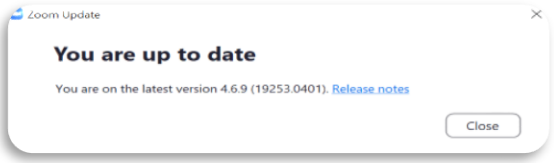
1. Make sure you are using the most current version of the Zoom application.
   Zoom releases security updates to protect those using the application. The most current version of Zoom should always be used to help protect everyone's security. If you are a Host, encourage the attendees you are inviting to do the same.

   To determine if you have the most current version on your desktop, follow these steps.

   1. Sign into the Zoom Desktop Client (Windows or macOS).
   2. Click your profile picture then click "Check for Updates".



3. Once you click on “Check for Updates”, it will notify you if you are on the latest version. If you are not, it will allow you to download and apply the latest update.



2. Don’t publicly share the meeting ID link on social media or any other public forum.

Security Tips for Hosts

1. Generate Automatic Meeting ID
   For meetings where you will be inviting many attendees or strangers, we recommend selecting “Generate Automatically” under the ID options for added security.
2. Be selective with sharing your PMI
   Anyone that knows your PMI can attempt to join any of your zoom meetings at any time. Invite with care and email or text the meeting ID link directly to the participant.
3. Use a meeting password
   Require participants to use a password so only those who have the password can join the meeting. You can enter any numeric password up to 10 characters.
4. Enable a waiting room for starting meetings
   This option has attendees stay in the waiting room until the host lets them in which they can do one at a time in order to screen for uninvited attendees and decline access for an attendee to pass from the waiting room into the meeting.
5. Review your security settings
   Continue for more detailed instructions.

How to Change Your Zoom Account’s Security Settings

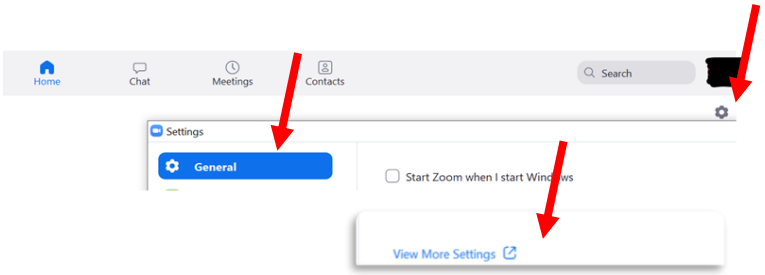
If you have a Zoom account, you can change your security settings through the Zoom portal. We strongly encourage hosts to review their Zoom settings prior to scheduling zoom meetings. How to access those settings are described below.

You can access the Zoom portal, a couple of different ways.

1. Go to the Zoom home page https://zoom.us and login using your account information is one option.

OR

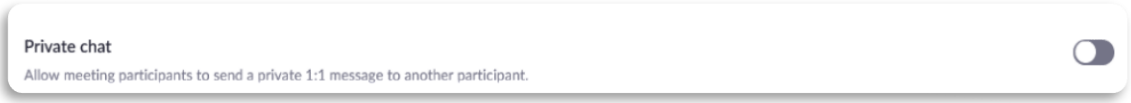
2. Go through your desktop application. In the upper right corner of your open zoom desktop application, click on the settings button. Once you click on settings, it defaults to the "General" tab. At the bottom of the "General" page, click "View More Settings" which will automatically take you to the Zoom portal.



The below settings we recommend changing can be found under: Personal | Settings | In Meeting (Basic)

1. Disable Private Chat

Disabling private chat eliminates the risk of having one attendee harasses another via private messaging. It also eliminates the risk of attendees talking about you, the Host, behind your back. When the button is gray, it's disabled.

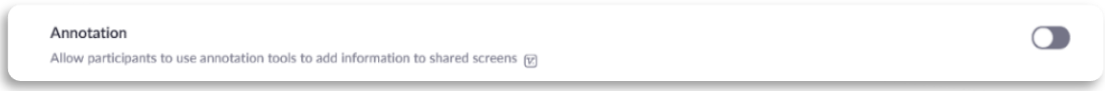


2. Limit screen sharing to Hosts

Hosts can prevent others from sharing their screens and videos by changing the screen sharing options to "Host Only."

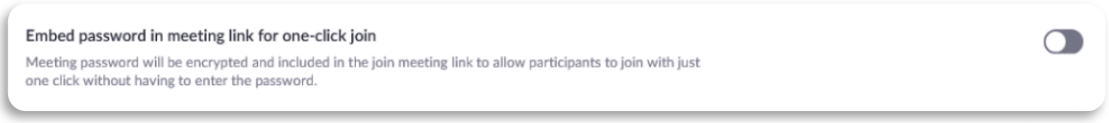
3. Annotation

Zoom has a feature that allows attendees to annotate the screen or image being shared which is great for collaboration. It might, however, provide an irresistible opportunity for an attendee to inappropriately collaborate. Annotation can be shutoff. When the button is gray, it's disabled.



4. Disable Embed Password

While Zoom provides an option to embed the meeting password in the Zoom meeting link to make it easier for attendees to join, it adds no additional protection if the Zoom meeting link is shared publicly. When the button is gray, it's disabled.



Reporting a Teleconference Hijacking

If you are a victim of a teleconference hijacking, or any cyber-crime for that matter, report it to the FBI's Internet Crime Complaint Center at ic3.gov. Additionally, if you receive a specific threat during a teleconference, please report it to tips.fbi.gov or call the FBI Cincinnati Division at (513) 421-4310.

Stay Tuned for Part Two….

The second part of this series will focus on additional security features that can be used during a meeting using the host controls.