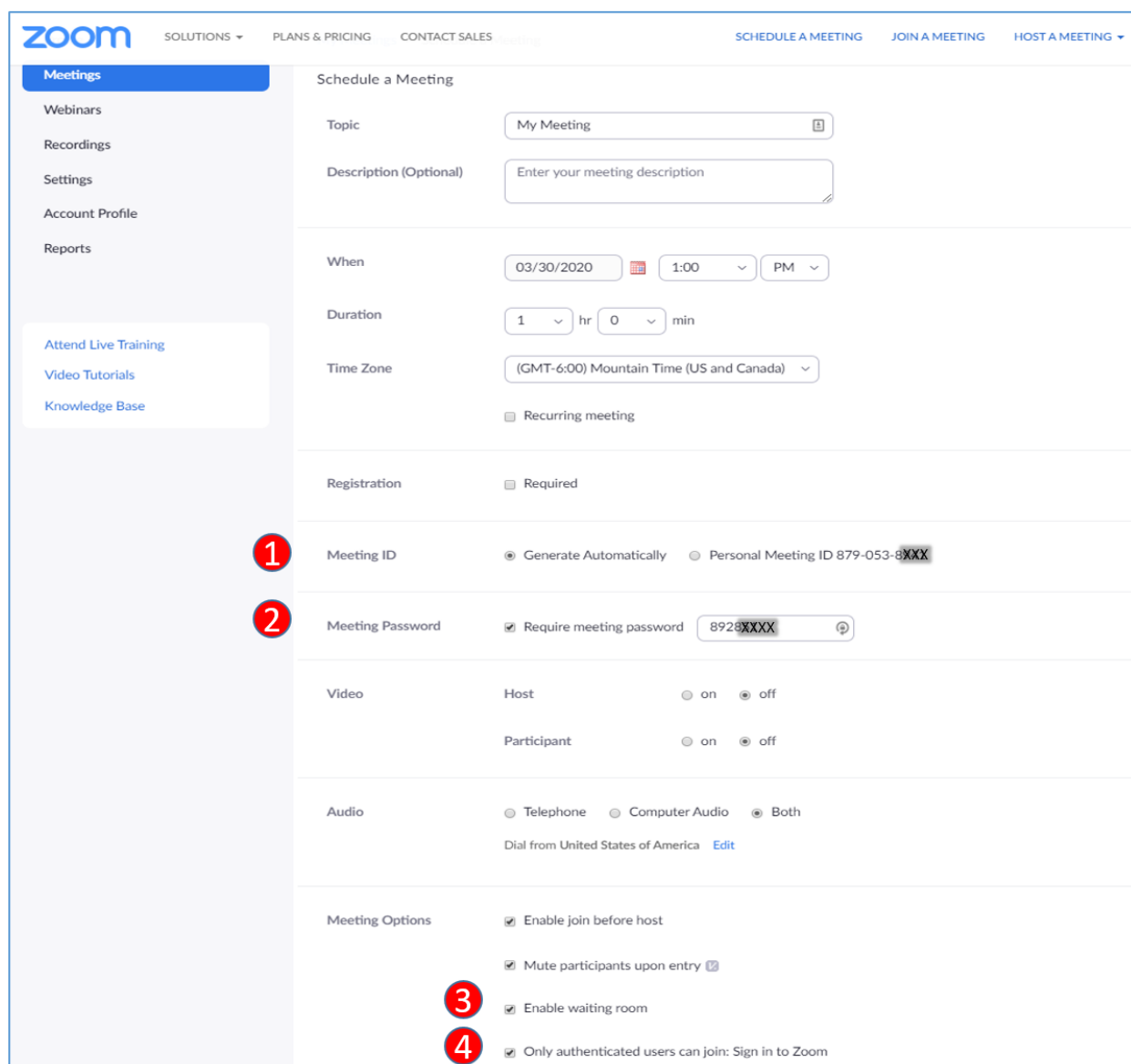


Protect your Zoom Meetings from Zoom-Bombings

Zoom-bombing is the term for uninvited guests that join Zoom meetings and disrupt the meeting by sharing violent and/or pornographic imagery, racist rants, hate speech or other comments meant to disturb the meeting participants. Although Zoom-bombing happens mostly on publicly available Zoom links, it can happen in other ways if your settings are not configured to protect against this. Here are ways to protect you and your guests from falling victim.

Before the meeting - make your meeting more secure

When scheduling your meetings, there are a few things you can do to minimize chances of Zoom-bombers. From the Meeting Scheduler section, consider the following settings:



The screenshot shows the Zoom Meeting Scheduler interface. The left sidebar contains navigation options: Meetings (selected), Webinars, Recordings, Settings, Account Profile, and Reports. Below the sidebar are links for Attend Live Training, Video Tutorials, and Knowledge Base. The main content area is titled 'Schedule a Meeting' and includes the following settings:

- Topic: My Meeting
- Description (Optional): Enter your meeting description
- When: 03/30/2020, 1:00 PM
- Duration: 1 hr 0 min
- Time Zone: (GMT-6:00) Mountain Time (US and Canada)
- Recurring meeting:
- Registration: Required
- Meeting ID: Generate Automatically, Personal Meeting ID 879-053-8XXX
- Meeting Password: Require meeting password, 8928XXXX
- Video: Host (on/off), Participant (on/off)
- Audio: Telephone, Computer Audio, Both (selected)
- Meeting Options: Enable join before host, Mute participants upon entry, Enable waiting room, Only authenticated users can join: Sign in to Zoom

1. Generate a random meeting ID instead of using your Personal Meeting ID (PMI) to host events. Your PMI is essentially one continuous (24/7) meeting and people can join at any time if they have the link.

Revised 4/1/2020

Platforms: Website for Online Learning, Infosec.byu.edu

Path: Box\Information Security\Training and Communications\Protect your Zoom Meetings.docx

Protect your Zoom Meetings from Zoom-Bombings

2. Add a password to the meeting. One of the best ways to add an extra layer of security to your meetings is to require the use of passwords to join.

There are a couple options to consider:

Option A: Setting a Meeting Password (not embedded in the link)

This is done at the meeting scheduler or meeting tab. You may configure the meeting password so that participants will need to click on the meeting link and enter the password to join.

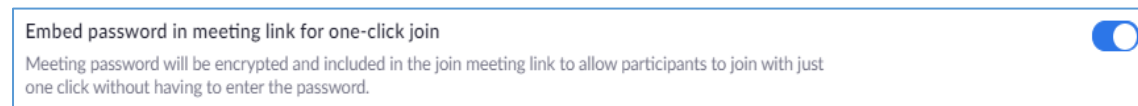
Note: You will need to send the link and password directly to attendees.

In the 'My Meetings, Schedule a Meeting' form, click the 'Require meeting password' checkbox and edit the password (or leave with the pre-filled password to use the auto-generated one). Once finished, click the Save button.

Option B: Enable One-click Passwords for Your Own Meetings

You may choose to enable use of one-click passwords. This setting is found at the Account level. This allows Zoom to generate meetings with the password embedded in the meeting link so that participants only need to click on the link to join and do not need to enter the password separately.

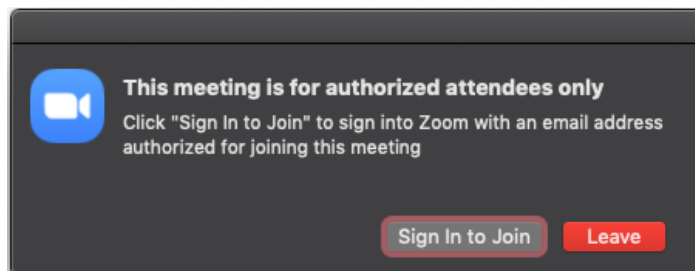
Note: You will only need to send the meeting link to attendees.



This is done at the Account Settings level. For instructions on how to enable this feature and additional information on passwords, refer to the [Meeting and Webinar Passwords](#) section on the Zoom Help Center.

3. Use the Waiting Room. This will allow you to see who has joined before you start the meeting. As this will require you to manually move people into your session, it works well for office hours or small groups, but it is not recommended for meetings with a large number of participants.
4. Only allow authenticated users to join. When this is selected, users have to be signed-in to their zoom.byu.edu account to join the meeting. If someone tries to join and isn't logged into Zoom with the email they were invited through, they will receive this message:

Protect your Zoom Meetings from Zoom-Bombings



Note: When using this option, you will need to communicate that those coming to the meeting will need to sign into Zoom first.

Finally, once you've set up the meeting, do not share your meeting link on social media or other public locations. Provide the link directly to specific people.

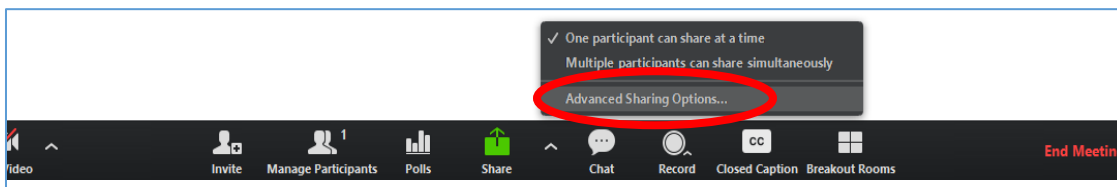
Learn how to schedule meetings by visiting the [Scheduling Meetings](#) page on the Zoom Help Center.

During the meeting – manage participants

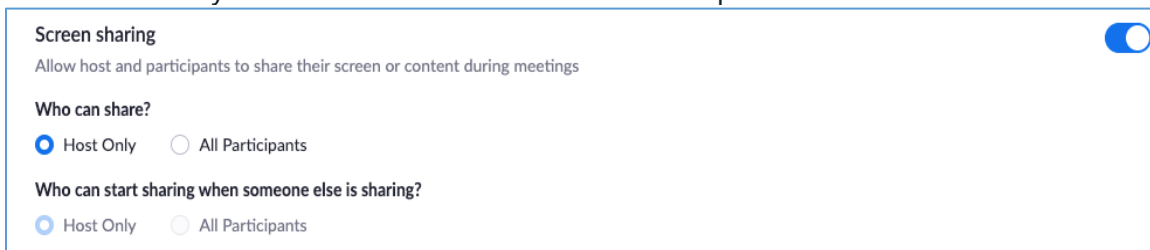
- **Manage screen sharing**

You want to be in control of the screen and what you are sharing. Prevent others from sharing unwanted content with the participants by restricting control of the screen sharing.

You can restrict this during the meeting in the host control bar. During the meeting, click the arrow next to Share Screen icon in the host control board (at the bottom) and choose Advanced Sharing Options.



Then select Only Host next to the 'Who Can Share?' question.



Revised 4/1/2020

Platforms: Website for Online Learning, Infosec.byu.edu


Path: Box\Information Security\Training and Communications\Protect your Zoom Meetings.docx

Protect your Zoom Meetings from Zoom-Bombings

- **Mute participants.**

You can mute/unmute individual participants or all of them at once. This will help you block unwanted, distracting, or inappropriate noise from other participants.

- **Stop Video.**

During the meeting you can turn off the participant's video camera by selecting *Manage Participants* on the control bar and clicking on the camera icon  next to their name in the participant list.

This helps you block and manage unwanted, disturbing or inappropriate gestures coming from the participant video camera. This does not prevent screen sharing (see *Manage screen sharing* above).

- **Turn off annotation.**

Do you need to have participants draw or annotate on your screen? Most meetings don't require this. You can disable the annotation feature in your Zoom settings to prevent people from 'high-jacking' your screen with unsolicited writing or drawings.



You will find directions for these settings and other ways to manage participants at [Managing Participants in a Meeting](#) on the Zoom Help Center.

With the increased use of Zoom as our primary telecommuting and tele-learning tool, it is important to reduce the risk of Zoom-bombing, unauthorized access to our meetings, and other intentional disruptions to our campus community.

Remember to use these Zoom meeting practices along with the [Work From Home](#) guidelines to help protect our information.

Tips from Zoom (March 20, 2020) *How to Keep the Party Crashers from Crashing Your Zoom*

Event: <https://blog.zoom.us/wordpress/2020/03/20/keep-the-party-crashers-from-crashing-your-zoom-event/>