How to Prevent “Zoom-Bombing:” A Guide

Many domestic violence coalitions and national technical assistance organizations have been worried about hosting meetings with colleagues via Zoom after hearing about “Zoom-bombings.” This is when malicious actors join and hijack a meeting by posting explicit content or just generally troll the meeting. This resource is designed to help those organizations adjust their settings to help secure against such events.

Please note – NNEDV has developed detailed guidance for victim service organizations considering using video platforms to provide direct services to survivors. See our Digital Services Toolkit at TechSafety.org for that information.

Preventing Unauthorized Access

REQUIRE REGISTRATION

This is an excellent option for deterring potential Zoom-bombers for two reasons. First of all, it requires extra steps to join the meeting, which can thwart less motivated bad actors. Second, it allows you to view everyone who registered and filter out any unrecognized or unusual registrants.

To do this, you can first login to https://zoom.us and either select “Schedule a New Meeting” (if you’re creating a brand new meeting) or find your existing meeting in the “Upcoming Meetings” tab.

★ If scheduling a new meeting, check the “Require Registration” box about halfway down the page.

★ If editing an existing meeting, first, you have to scroll down on the “Manage [Meeting Name]” page and find “Edit this Meeting” (bottom right). On the edit page, you’ll see the “Require Registration” checkbox.
Don’t forget to save once you’ve turned on registration!

After you’re back to the meeting’s management page (which will come up after you’ve finished scheduling or editing), if registration is turned on, there will be a new section at the bottom of the page, where you can edit registration settings. Click “Edit” next to “Automatically Approve,” as seen below:
And now you’ll have a choice to make: **automatically approve** registrants or **manually approve** registrants. We recommend **manually approving** registrants. While this might *seem* like a pain, it’s actually quite easy to approve in large batches (more info later).

We also suggest closing the registration after the event date and not showing social share buttons. Here’s a screenshot of the recommended settings:
You can add questions to the registration that you might want your potential participants to answer. This could be useful to help you guide the meeting or even just to get more information about who will be in your meeting. Zoom gives you a list of sample questions, and you can add your own custom questions. You can make any number of them required by checking the box on the right hand side.

To invite attendees to your webinar, you’ll be given a registration link that you can share. You can either just copy the invitation, which copies some
boilerplate text that Zoom uses, or you can copy the URL and share with your own message.

Once people have started registering for your meeting, you can review and approve the registrants. Note that even if you don’t have manual approval turned on, you can still cancel a registrant and their unique “Join” link will no longer work. Here’s where you can review and approve registrants:
If you have multiple registrants and you just want to select them all to approve, you can click the checkbox at the top left of the list, then click “Approve.” By clicking on the person’s name, you can also review their answers to registration questions.

If you need to deny a registrant, you have the chance to edit the message that’s sent. This is a good way to say something like “Sorry, we’re over capacity for this meeting, but we’ll schedule another or send a recording.”
You’ll always be able to review the approved registrants on the “Approved” tab and cancel some (or all) registrations. This works because, unlike a regular Zoom join link, each person receives a *unique* link to join. If their registration has been cancelled, their link will not let them join.

**Note: Registrants should NOT share their join link with others.** When two people join from the same link, they’ll both join with the same name. They will also count as two participants, which could cause attendance to exceed the number of attendees permitted with your license.

**USE A UNIQUE ID FOR LARGE/PUBLIC ZOOM CALLS**

When you host a meeting in Zoom, you may want to use your Personal Meeting ID. This is an ID that is static and assigned to your account, which can make it really easy to set up and join standing meetings or weekly check-ins with colleagues.

However, if you’re hosting a meeting where members of the public or other strangers are invited, we recommend using a Unique ID. Once you put your Personal Meeting ID out to the world, anyone can jump into any future meeting you set up using that ID. Here’s how you set up a meeting with a Unique ID:

- In the Zoom app, create a new meeting. This window will appear:
Select “Generate Automatically” and Zoom will provide you with a Unique ID for this meeting.

**USING A MEETING PASSWORD**

Above, you’ll see we also pointed out the checkbox to require a meeting password. This is only an option when you generate a unique ID. Adding a password will create an extra layer of security for your Zoom meeting. You’ll
have to distribute the password to those who have replied to the RSVP and seem credible.

**CREATE A WAITING ROOM**

Another way to screen people before they join the Zoom call is to create a waiting room. When participants join the meeting, they’ll be greeted with a waiting room screen and won’t be in the call until the host decides to let them in. The host can let people in all at once or one at a time, which lets the host screen for unrecognized individuals.

To turn this setting on or off, login to [https://zoom.us](https://zoom.us) in a web browser. Go to “Meetings” and click on the meeting you want to enable a waiting room for. Click “Edit this meeting” and scroll down to “Meeting options.” You’ll see these options:

<table>
<thead>
<tr>
<th>Meeting Options</th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Enable join before host</td>
<td></td>
</tr>
<tr>
<td>Mute participants upon entry</td>
<td></td>
</tr>
<tr>
<td>Enable waiting room</td>
<td></td>
</tr>
<tr>
<td>Only authenticated users can join</td>
<td></td>
</tr>
<tr>
<td>Record the meeting automatically</td>
<td></td>
</tr>
</tbody>
</table>

You’ll be able to toggle the waiting room settings here.

**Additional Steps in Case a Bad Actor Enters your Zoom Meeting**

Even with the best laid precautions, it’s possible someone you don’t want in your meeting might find their way in. The following steps can be used if someone unexpected enters your meeting.

**MAKE SURE ONLY HOSTS CAN SHARE THEIR SCREENS**

Should a bad actor somehow make their way into the meeting, you’ll want to prevent them from totally hijacking your meeting. Step one for that is to prevent them from sharing their screen. You can do that in advance of your meeting. Again, login to zoom.us in a web browser. Navigate to Personal > Settings > In Meeting (Basic). Scroll to Screen Sharing and you’ll be able to toggle sharing permissions here:
Change it to “Host Only,” that way no one can hijack the screen and share unsavory content.

**LOCK A MEETING ONCE IT STARTS**

Once you start a meeting, and everyone you expect to join is in, you can lock the meeting to prevent anyone else from joining. While the meeting is running, navigate to “Manage Participants” at the bottom of the screen. This will open a panel on the side of your window. At the bottom, choose “More” then “Lock Meeting.”

**KICK SOMEONE OUT OF THE MEETING**

If a malicious actor enters your meeting, you still have the ability to remove them. To kick them out, navigate to ”Manage Participants” as above. Hover over the name of the person you want to kick, and when options appear, select “Remove.”