Zoom Security Recommendations

Passwords don't prevent Zoom Bombing! Don't get bombed.

Many Zoom meeting considerations need to be reviewed ***before you even begin to publicize your event*.** The information below is meant to help you to make meetings more secure and address any problems that may arise during a meeting. This document addresses meetings as they are most commonly used. A Zoom Webinar may provide additional security measures but differs in functionality from a meeting. There is no way to completely eliminate the risk of unwanted activity in your Zoom meeting, but the following recommendations can reduce the chance of unwanted interruptions. Be sure to read the entirety of this document prior to marketing your event.

The Digital Education and Innovation team is happy to meet with you as you plan your event to help you consider and apply appropriate security measures. Please email deiteam@umn.edu.

Before the Meeting

Basic Security

All UMN Zoom meetings by default have one of the following enabled for scheduled meetings:

- **Password** - Passwords add extra security encryption, but if the URL with password is shared widely, they offer no additional protection.
- **Waiting Room** - Enabling the waiting room requires the host of the meeting to individually admit participants as they arrive. If you have a specific guest list, this can be an easy way to ensure only intended participants enter the meeting. The host can send messages to those in the waiting room (example: "Please change your username to your real name") if needed.

Read more about Basic Zoom Security.

Additional Security Measures

The following options will make it more difficult for unwanted participants to enter your meeting, but are not foolproof:

- **Require authentication to join** - Only participants with authenticated Zoom accounts, which can be limited to UMN Zoom accounts, are permitted to enter the meeting.
    - If you know all your participants will be joining from within the UMN system, this will help prevent outsiders from joining. Read more about only allowing Authenticated UMN users here.
    - Read more about authentication including allowing exceptions for guest speakers or guest attendees from outside of the UMN.
- **Meeting Registration** - Registration will require participants to sign up for the meeting and obtain the link from a valid email address. There are several registration options:
    - Automatic Approval (less secure) - Anyone who signs up will be approved and receive information on how to join.
    - Manual Approval (more secure) - Anyone who signs up will need to be approved by the host on the meeting management page, and then will receive information on how to join. Any registrants still *Pending* at the time of the meeting will not be able to join.
    - Read about other registration options.

Recommendations

Think carefully about your audience members.

- If you are expecting a relatively unfamiliar audience or are advertising widely and publicly, enabling authentication or registration can deter unwanted guests.
- If your audience is known, using Manual Registration Approval will ensure only your wanted guests will be part of the meeting.
- If you do not advertise publicly, you limit your exposure and reduce your chance of an interruption (but the risk is not completely eliminated).

Read more about in-meeting security options.

As the Meeting Starts

Once your event has started, you may choose to use the following features to keep new, potentially unwanted participants, from entering:

- **Enable Waiting Room** - From the security button, hosts can enable the waiting room. New attendees will be put into a waiting room. The host will be notified that there are people waiting and will display that person's Zoom

username and their email address, if provided. The host can then choose to admit that person. This is helpful in the case of multiple bad actors trying to Zoom Bomb a meeting all at once. Read more about waiting rooms.

- **Lock Meeting** - From the security button, hosts can choose to lock the meeting. When you lock a Zoom Meeting that has already started, no new participants can join, even if they have the meeting ID and passcode. Read more about locking the meeting.
- **Customize Security Settings** - Click on the "Security" button. Check or uncheck the options under "Allow Participants to:" so your audience can participate in the way you expect them to.

Recommendations

Think about your audience participation in the meeting.

- Have a defined plan for how participants will be addressed if they need to leave the meeting and return or if they will be late. This may be to utilize the waiting room. If no one is expected to leave and return, lock the meeting.
- If unknown people enter at the beginning of the meeting, interact with them in a welcoming way to see if they are part of your intended audience.
- Consider a co-host or alternative host to assist as the meeting begins. This individual can monitor the waiting room, the chat, and other in-meeting settings.
- Create a checklist of expected participant interactions and customize the meeting's settings accordingly.
- If you have only a few primary speakers, consider making them co-hosts and turn off audio and/or video for others until it is time for them to interact.

Emergency Action In Meeting

If you experience Zoom Bombing, use the following steps to stop the disruption quickly and regain control over the meeting:

1. **Suspend all participant activities** - Click on "Security" and then select "Suspend All Participant Activities". This will immediately:
    - Disable everyone's audio
    - Disable everyone's video
    - Stop all screen sharing
    - Disables everyone's use of chat
    - Hides participant's profile images
    - Locks the meeting to prevent any new participants from entering

2. **Communicate with your audience** - Unmute yourself, explain that there has been a disruption in the meeting and you are resolving it. **At this time all attendees will not be able to unmute themselves, start their video, or type in the chat.** Only hosts and co-hosts of the meeting can un-mute themselves and start their video.
    - If someone other than the meeting host or co-host needs to speak, you can ask individuals to unmute themselves by hovering over their name in the participants panel or hovering over their square on the gallery view and clicking "Ask to Unmute." There is no way to ask participants to start video, screen sharing, or chat use while participant activities are suspended.
3. **Remove unwanted participants** - There are three ways to remove a participant. It does not matter which you choose.
    - Hover over the participant's image while in gallery view, click on the three dots, select "Remove" from the bottom of the list.
    - In the participant panel, hover over the participant's name, click "more," select "Remove" from the bottom of the list.
    - Click on "Security," click on "Remove Participant…," click on "Remove" next to the name of the participant.
4. **Re-open your participant options** - Once the unwanted participant(s) have been removed, it is recommended that the meeting remain locked. You can re-open the options for participants to unmute themselves, use video, use the chat, and screen share by checking those items in the "Security" section.

Read more about in-meeting security options.

Recommendations

Be prepared to address Zoom Bombing in your meetings.

- Familiarize yourself with the options listed above in advance. If unwanted actors join your session, it can feel chaotic and speed is helpful in removing the problem individuals.
- Consider a short note in your registration materials as to what might happen if issues arise in meetings, especially if your event is public.
- If you are unfamiliar with Zoom settings, review them at zoom.us/test or sign up for a consultation with a member of the Digital Education and Innovation team by emailing deiteam@umn.edu.

- Consider having a co-host to assist you with larger events, especially if they have been advertised publicly.
- Unwanted actors may also appear in your meeting breakout rooms. Keep your breakout rooms secure by:
    - Locking your meeting before opening breakout rooms.
    - Assigning a co-host to be in each room and remove people if needed.
    - Pop in occasionally to assure all is going as planned.
    - Make sure your participants know they can request for help by using the "Ask for Help" button while in a room.

Zoom Security FAQ

Can I set up some security measures ahead of time, before the meeting starts?

- Yes. By default, University of Minnesota zoom meetings already require either the waiting room option or a passcode to be enabled. You can check those on your profile. Read more about Adjusting Your Settings for a More Secure Meeting.

I am using Zoom for my online class, with no guest speakers. What should I do?

- Before your class meeting, you can select that only University of Minnesota Accounts can log in to your class meeting. Read more about Adjusting Your Settings for a More Secure Meeting.
- Once everyone in your class has joined, enable the waiting room.

I am using Zoom for a job talk or with a guest lecturer where I need non-University of Minnesota participants to join. What should I do?

- The most secure route would be to have participants register for the event in advance. You can learn how to set up registration for your event (meeting or webinar).
- Enable the waiting room 10 or 15 minutes after the event start time to handle any latecomers. You can click on the security button at the bottom and select to enable the waiting room.
- Lock the meeting. You can click on the security button at the bottom and select to lock the meeting.

My class is being Zoom Bombed right now. What should I do?

- The host of the meeting should Immediately click on "Security" and then select "Suspend All Participant Activities". This will disable everyone's audio, video, chat, and the participant's user image.

- The host can then unmute themselves and start their video to explain the incident. They can then choose to end the meeting or eject the unwanted participants.

I want to share my URL publicly, is that okay?

- Posting a link to your meeting on Twitter, Facebook, Reddit, or anywhere publicly available to the Internet makes your meeting inherently insecure and more likely to be Zoom Bombed. This is not recommended. If you want to invite members of the public, consider having registration set up beforehand.

Help us improve our resources. Take this one-minute survey.