MINNESOTA STATE

Ways to secure your Zoom meetings?

CONTENTS

Originally published on March 31, 2020 • Version 2.0 last updated on April 1, 2020

WHAT IS ZOOMBOMBING?

"Zoombombing" has been a term used to describe when participants, typically uninvited, join a Zoom meeting with the intention of deliberately disrupting a meeting. This has resulted in uninvited participant(s) (1) sharing their screen which includes offensive material, (2) using the annotation tool to include unwanted annotations, typically offensive in nature, (3) adding unwanted messages/files in chat that are often offensive or links to offensive websites, and/or (4) interjecting with video and/or audio that includes offensive audio and/or video.

WHAT IS ZOOM AND MINNESOTA STATE DOING TO SAFEGUARD MEETINGS?

Noting "privacy and security of our customers is our top priority," Zoom has enforced two critical changes to the account defaults for all education customers using the Zoom meetings platform. These changes were applied to the Minnesota State platform on April 1, 2020 and those whom administer the Minnesota State Zoom service intend to follow Zoom's guidance by keeping these settings as the default for all new users or newly created meetings on our managed service (https://minnstate.zoom.us). Like most settings in Zoom, as an individual host you have the ability to change settings for all your meetings at https://minnstate.zoom.us/profile/setting or by editing the individual settings for a meeting.

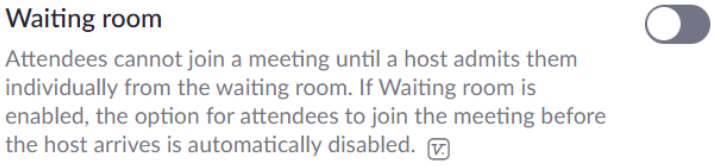
Default Setting Change 1: Waiting Rooms Enabled for Guest Accounts (Began on 4/1/2020)

Participants who have logged in to Zoom via SSO (single sign on) at https://minnstate.zoom.us using their StarID and password will join a meeting and bi-pass the waiting room. Participants who haven't logged in Zoom via SSO (single sign on) before attempting to join a Zoom meeting are identified by Zoom as a "Guest." As a "Guest," these participants will be placed into the meeting's waiting room until a Host (or co-host) of the Zoom meeting chooses to allow those display names they recognize to join the Zoom meeting.

Want to change this default setting?

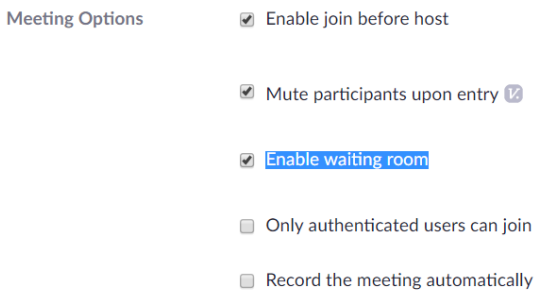
Option 1: Change settings for all your meetings

1. Go to https://minnstate.zoom.us/profile/setting. This changes settings for all meetings associated with your account.
2. Locate the **Waiting room** setting located under **In Meeting (Advanced)** section and turn off the setting.



Option 2: Change settings for an individual meeting, or edit an existing meeting

1. Go to https://minnstate.zoom.us/meeting/schedule, or edit an existing meeting
2. Under **Meeting Options** heading, choose **Enable waiting room**



What are the considerations if I change this setting?

a. Can be tedious for hosts: There is an option to "allow all" participants from a waiting room into a meeting, but it can be tedious for a host to monitor who is currently in the waiting room and selecting the option to allow the participant.
b. Can be confusing / anxiety inducing for Participants: As a participant attempting to join a meeting, you are expecting to join a meeting, but you'll be presented with a message (albeit a configurable message by the host) that they are in a waiting room and must wait for the host to allow them into the meeting.
c. Limiting a waiting room to guests: You can select the option in your waiting room to allow individuals who have signed in (with their Star ID) to bypass the waiting room. This can improve the overall experience, but you may run into issues for participants/student using single sign on as outlined in Option 4.

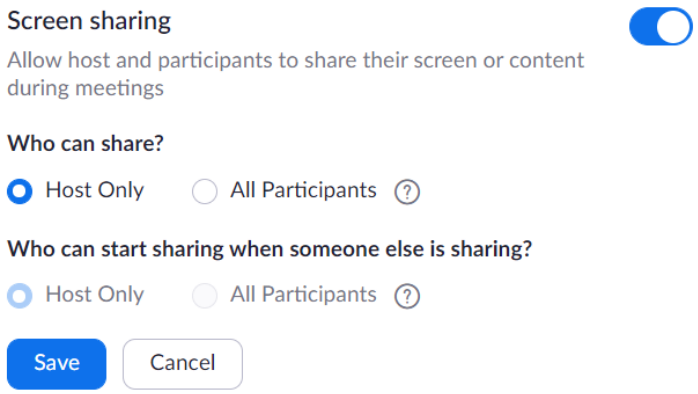
Back to the top

Default Setting Change 2: Only hosts can share

Only those who are logged in as the host or co-host of a Zoom meeting will be able to share their screen with meeting participants/students. The host of the meeting will now need to allow participants with the ability to share their screen.

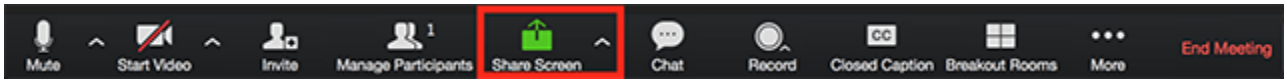
Want to change this default setting?

1. Go to https://minnstate.zoom.us/profile/setting. This changes settings for all meetings associated with your account.
2. Locate the **Share Screen** setting located under **In Meeting (Basic)** section and select **Host Only** or **All Participants**.



How do I change this setting while a meeting is in progress?

1. In the host controls, click the arrow next to **Share Screen** and click **Advanced Sharing Options**.



2. Under **Who can share?** choose **Only Host** or **All Participants.**
3. Close the window.

Source: Zoom: Managing participants in a meeting

What should I be aware of, with this change this setting?

a. **If you are not the host**: You may join a meeting for which you are supposed to be the host, but you launched Zoom and you weren't signed in as the "host." Because Zoom doesn't recognize you as the host, you will not be able to share your screen – as Zoom is only allowing the host of a meeting the option to share. See how to claim host privileges if you are in a Zoom meeting and supposed to be the host.
b. **Participants Can't Share**: If you want a participant in your meeting to share their screen, you will need to promote them to co-host and/or change your sharing permissions while your meeting is running.
c. **Vulnerabilities still exist**: Because participants still can use their webcam, unmute themselves and/or use the chat tool, an unwanted participant can still broadcast unwanted audio/video and/or post unwanted messages via the chat. Although you can prevent, participants from using their audio and chat, you will be limiting the ability for participants to actively participate to a Zoom meeting.\

Back to the top

SHOULD I BE CONCERNED ABOUT ZOOMBOMBING

In most cases, meetings that have been "Zoombombed" have occurred when a link to a Zoom meeting has been placed on a public online location (e.g. posted to a publicly accessible website or via publicly available social media posts). Just like search engines (Google, Bing, etc.) locate content online, individuals with nefarious intentions have programmed (ro)bots to scour the internet looking for references to join Zoom meetings. Once locations of Zoom meeting locations are known, these individuals join Zoom meetings at the specified times with the intention of creating havoc within a meeting, often by introducing offensive content to all participants.

Back to the top

CAN I PREVENT ZOOMBOMBING FROM HAPPENING TO MY MEETINGS?

In most cases, when you limit the locations where you post links to your Zoom meetings, you reduce the risk that a meeting you are hosting will be Zoombombed. This can be done simply by choosing to limit the locations in which you share your meeting location with participants/students. For instance, providing a link within a D2L Brightspace course site or emailing a link directly to your participants/students, limits the likelihood that a (ro)bot will locate your Zoom meeting location. Additionally, to comply with the Federal Education Rights and Privacy Act (FERPA) it is always best to limit information about how to access your course to those who are

enrolled in in your course. As the host of a meeting, you can limit where you choose to share a link to your Zoom meeting location.

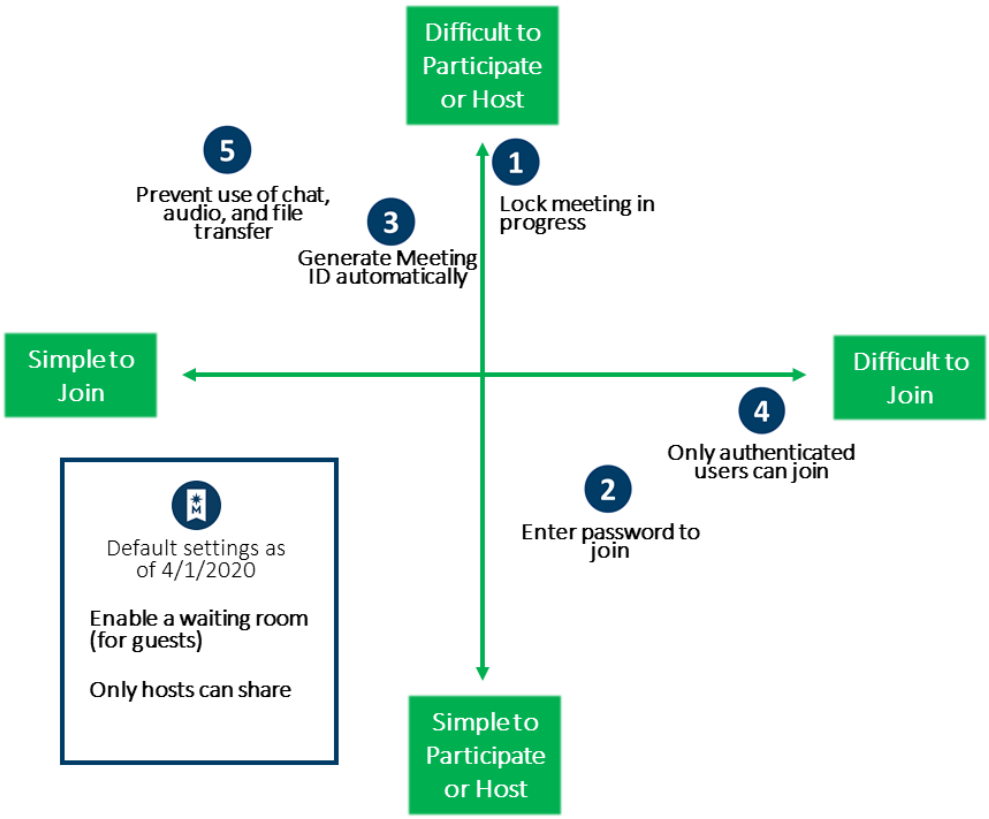
Back to the top

ADDITIONAL SETTINGS TO REDUCE THE LIKELIHOOD THAT YOUR MEETING WILL BE ZOOMBOMBED

If you are concerned that a Zoom meeting you are hosting will be Zoombombed, you can add some of the options included below in the infographic. The current defaults for Zoom meetings at https://minnstate.zoom.us were set in consultation with the Media Management and Web Conferencing committee. These defaults were set to reduce the barriers for students to join and to increase the opportunities for all participants to actively contribute during a meeting.

You can use more than one of the options below, but as noted in the infographic, the more options you add to your Zoom meetings the more complex it becomes for your expected participants/students to join and/or for participants/hosts to participate in a Zoom meeting.

Figure 1. Zoom settings to reduce Zoombombing



Back to the top

WHAT SHOULD I DO IF I AM THE HOST OF MEETING THAT IS BEING/HAS BEEN ZOOMBOMBED?

For those who have experienced a meeting that has been "zoombombed," the experience can be so disturbing it becomes hard for a host to know how to intervene technically.

While Zoombombing is occurring?

If you can maneuver quickly, you can take the following steps.

1. Locate the uninvited guest in your participant list and choose the option to remove them, then "Lock" your room to avoid repeated attempts by the unwanted participant to return.
2. There may be some residual offensive content left by your Zoombomber. With the Zoombomber gone, participants shouldn't see their shared screen. If annotations were made on a screen or whiteboard, you can clear all annotations. Unfortunately, if offensive material or files were added to the chat, you are unable to remove previously posted content as a host.
3. You can choose always choose to "end meeting" for all participants, create a new meeting with a randomly generated meeting ID and provide your participants with this new link somewhere private (e.g. via email or through D2L Brightspace)

After you've been Zoombombed?

1. If it was your personal meeting location that was Zoombombed, you can change your personal meeting ID to a new 10 digit code. Directions available from Zoom.
2. If you created the meeting, delete the meeting and create a new meeting location to share with participants. Be sure to limit where you publish the link to your Zoom meeting. See directions from Zoom.

Back to the top

OPTION 1: LOCK MEETING TO ADDITIONAL PARTICIPANTS AFTER START OF MEETING

You can lock the meeting to prevent additional participants from joining, even if they have your meeting ID and password (if you set one).

How does making this change reduce my risk?

Once your meeting has started and you know that you have all the appropriate participants/students in your Zoom meeting, locking your meeting will stop any participants from joining your meeting.

Why isn't this already set as a default.

There is no option to lock your meeting after X minutes of when it starts. Zoom requires someone with host permissions to "Lock" a meeting room.

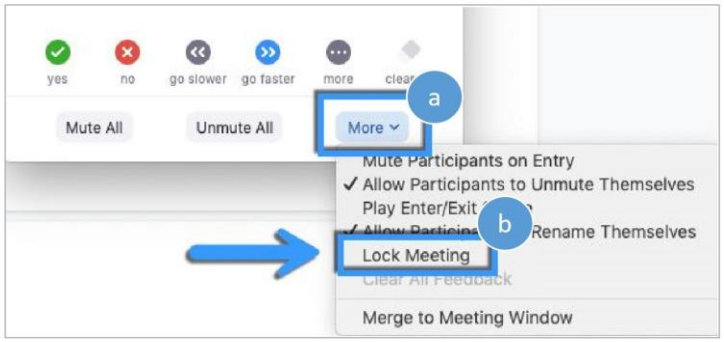
How do I set this up?

How do I change this up for all my meetings?

This option is not available to setup until a meeting is in progress.

How to change this setting while a meeting is in progress.

1. In your **Zoom application** (Windows/Mac), navigate to the **Participants Panel**
2. Select **More** ˅ and choose **Lock Meeting**



What are the considerations if I change this setting?

a. You may be locking out students that are late: Once you lock your meeting, no one can join, including a student that may be running late. Requiring that all your participants/students must be in your room by a specific time may not be the most considerate requirement of students/participants. Who among us haven't been late to a meeting in our life?

b. You may be locking out students that need to exit/re-join for technical reasons: If a student is experiencing a technical issues while a meeting is progress. The may need to leave the meeting and rejoin. If your meeting is locked, they aren't provided with the option to re-join. If they are already experiencing technical issues, they may not be able to communicate they need to leave and re-join/unlock the room.

Back to the top

OPTION 2: ADD A PASSWORD TO JOIN A ZOOM MEETING

When participants attempt to join a meeting, they will be prompted to enter a password that you, as the host, have set and discretely communicated (e.g. via your D2L Brightspace course, via email, via SharePoint) to your participants.

How does making this change reduce my risk?

If the link to your Zoom meeting location has been published to a publicly accessible website, you can share the password to join your meeting with your intended participants only.

Why isn't this already set as a default?

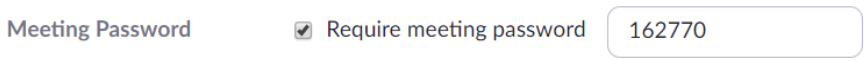
Locating the correct link to join a Zoom meeting can be challenging enough for some participants, when you add in a password that must be entered, your participants need to locate this additional piece of information.

How do I set this up?

How do I set this up for all my meetings?

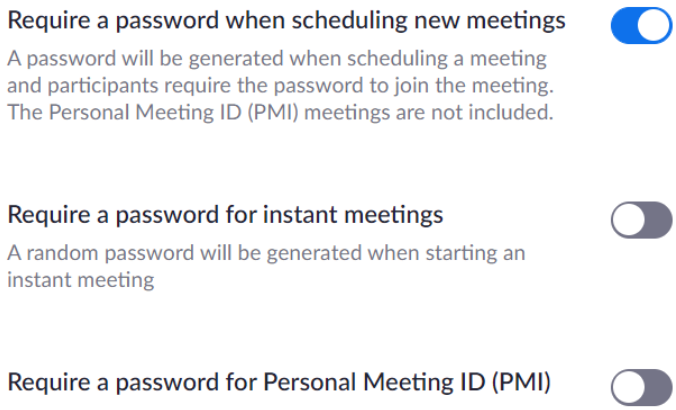
Option 1: Require a password when scheduling a meeting, or edit an existing meeting

1. Go to https://minnstate.zoom.us/meeting/schedule, or edit an existing meeting
2. Under **Meeting Password** heading, select **Require meeting password** and enter a password.



Option 2: Change this setting for all meetings

1. Go to https://minnstate.zoom.us/profile/setting. This changes settings for all meetings associated with your account.
2. Locate the **Require a password when scheduling new meetings** and/or the **Require a password for Personal Meeting ID (PMI)** setting located under **Schedule Meeting** section and turn on the settings.



How do I change this setting while a meeting is in progress?

This option does not exist while a meeting is in progress.

What should I be aware of, if I change this setting?

a. Passwords are case sensitive: Use something easy enough. Directing participants to enter, “PassWord” is different than a partipant entering “password”
b. Characters can be visually confusing: Depending on the font type, characters can be confusing to discern, “IW0RD” is the an uppercase ‘i’ and you’ll see ‘0’ is a numeral, not the letter ‘o’

Back to the top

OPTION 3: CREATE A RANDOM LOCATION FOR EACH COURSE OR MEETING

When you schedule a meeting have Zoom randomly generate a meeting ID.

How does making this change reduce my risk?

If you are regularly using the same Zoom meeting location for all your meetings (e.g. personal meeting room) you are increasing the likelihood that the location of your meeting will be distributed to places outside of your control. By providing participants with a randomly generated meeting ID, you are reducing the availability to join your meeting.

Why isn't this already set as a default?

Many hosts like to provide a "persistent" link to a meeting location that occurs with regular frequency. For instance, a faculty member may want to communicate one meeting location that students can join for their "office hours." Or, a faculty member wants to communicate students, for the duration of term, a link for all synchronous class meetings will be https://minnstate.zoom.us/j/MY-X-CLASS for "Class X" and https://minnstate.zoom.us/j/MY-Y-CLASS for "Class Y." Creating a unique link for each meeting as a host can be time consuming and locating the correct link for each meeting can be confusing for participants/students.

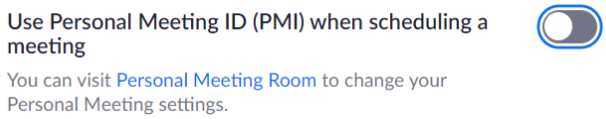
How do I set this up for all my meetings?

Option 1: Generate Automatically when scheduling a meeting

3. Go to https://minnstate.zoom.us/meeting/schedule
4. Under **Meeting ID** heading, choose **Generate Automatically**.

Option 2: Change your account settings to default that a new link be created.

1. Go to https://minnstate.zoom.us/profile/setting. This changes settings for all meetings associated with your account.
2. Locate the **Use Personal Meeting ID (PMI) when scheduling a meeting** setting located under **Schedule Meeting** section and turn on the settings.



How do I change this setting while a meeting is in progress.

This option does not exist while a meeting is in progress.

What should I be aware of, if I change this setting?

a. Time Consuming for Hosts: Creating a unique link for each meeting as a host can be time consuming
b. Confusing for Participants: Locating the correct link for each meeting can be confusing for participants/students.

Back to the top

OPTION 4: ONLY SIGNED-IN USERS CAN JOIN

Require your participants/students to sign-in with their StarID and password.

How does making this change reduce my risk?

By require your participants/student to sign-in with their StarID and password before joining a meeting, you know that your participant is associated with a Minnesota State institution.

Why isn't this already set as a default.

Like other higher education institutions, Minnesota State provisions feature rich, professional level accounts to Zoom for students, faculty, and staff affiliated with Minnesota State by using something called a "single sign on" service, or SSO for short. Rather than having to remember a unique email and password to access services like Zoom or Kaltura, Minnesota State individuals can access these services by entering their StarID password when prompted by our SSO service.

Confusing Log in messages in Zoom: As a popular international service used by many individuals, many experiences in Zoom direct individuals to login with their email address and password. If you are novice user, you must look closely for the option to sign in with SSO. Additionally, as a novice user it is unlikely you know that you have to use SSO to login.

Associating Personal Accounts with Minnesota State Zoom: Zoom uses an individual's email as the unique identifier for all users. Finally, individuals who have already created an account using their institutional email at Zoom.com or Zoom.us, prior to attempting to login at https://minnstate.zoom.us, upon the individuals first login, Zoom will require the individual to complete a couple of steps by responding to an auto-generated email to their account. All of which can

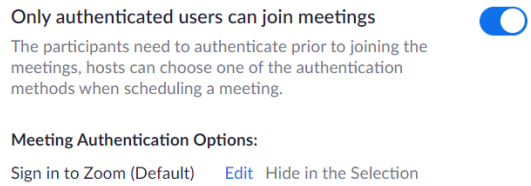
Limiting access to External Participants: Some faculty/hosts want to invite guest speakers and/or individuals not affiliated with a Minnesota State institution (no StarID) to participate in a Zoom meeting. Applying this setting limits the access to this service to any external participants.

How do I set this up?

How do I set this up for all my meetings?

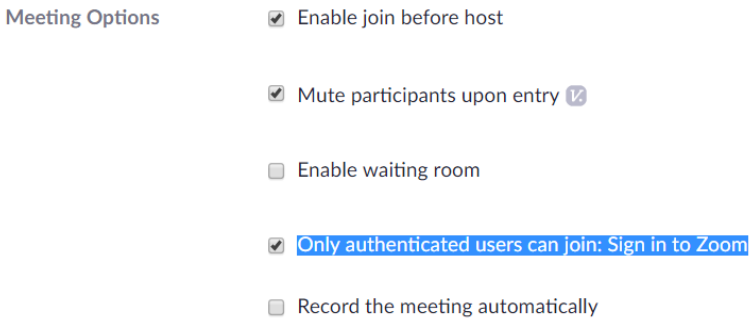
Option 1: Change settings for all your meetings

1. Go to https://minnstate.zoom.us/profile/setting. This changes settings for all meetings associated with your account.
2. Locate the **Only authenticated users can join meetings** setting located under **Schedule Meeting** section and turn on the settings.



Option 2: Change settings for an individual meeting or edit an existing meeting

1. Go to https://minnstate.zoom.us/meeting/schedule, or edit an existing meeting
2. Under **Meeting Options** heading, choose **Only authenticated users can join**



How do I change this setting while a meeting is in progress.

This option does not exist while a meeting is in progress.

What are the considerations if I change this setting?

Refer to the section above that describes why this setting is not already a default.

Back to the top

OPTION 5: PREVENT PARTICIPANTS FROM USING AUDIO, CHAT, FILE TRANSFERS…OR JUST USE ZOOM WEBINARS?

If you are anticipating your meeting to be uni-directional in which you, as the host, are only disseminating information to participants/students with no/limited interaction, you can prevent the tools in Zoom that allow for participants to interact.

How does making this change reduce my risk?

By limiting participant access to use these tools, you dramatically remove the ability for participants to interact with one another in Zoom.

Why isn't this already set as a default?

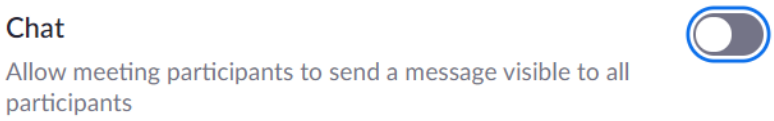
Zoom is a collaboration platform. Most people elect to use this service because they want to provide their participants with options to easily contribute to the meeting whether it is through their audio, video, or chat. Although the host can allow these options per user or tool, it can be very disorienting to participants who are expecting to be able to use these core features of a web conferencing platform.

How do I do set this up?

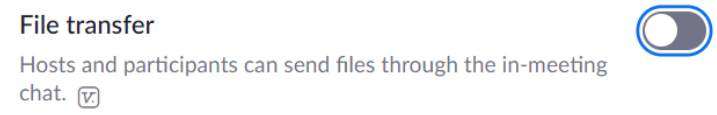
How do I set this up for all my meetings?

Option 1: Change settings for all your meetings

1. Go to https://minnstate.zoom.us/profile/setting. This changes settings for all meetings associated with your account.
2. Locate the **Chat** setting located under **In Meeting (Basic)** section and turn off the settings.



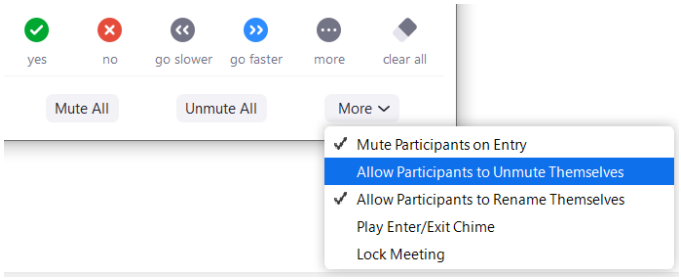
3. Locate the File transfer setting located under **In Meeting (Basic)** section and turn off the settings.



How do I change this setting while a meeting is in progress.

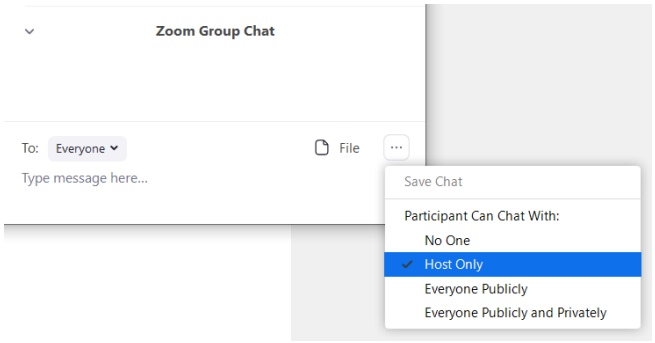
For audio

1. In your **Zoom application** (Windows/Mac), navigate to the **Participants Panel**
2. Select **More** ˅ and choose **Allow Participants to Unmute Themselves**



For chat

1. In your **Zoom application** (Windows/Mac), navigate to the **Chat Panel**
2. Select **. . .** and choose **Host Only** under Participant Can Chat With:



You can't prevent participants from sharing their video or using the file while a meeting is in progress.

What are the considerations if I change this setting?

a. Total Confusion: Participants that join a web conference typically expect they have the access to contribute, whether via audio, video, or chat. You'll want to communicate to participants/students about how you have limited the functions.
b. Webinars: All employees (faculty and staff) affiliated with Minnesota State have access to use the Zoom webinar tool. The default tools and features of the webinar tool is designed to limit interaction among participants without the intervention of a host. For instance, without granting permissions, only the "panelist" and "host" can share their screen, use audio, and use video. Additionally, you can limit the chat tool so message are sent only to the host or panelist of a webinar. Due to the limited interactions afforded through a webinar, Zoom webinars (rather than Zoom meetings) are better suited if you intend to have a uni-directional meeting.

Back to the top

MORE COVERAGE OF ZOOMBOMBING

1. FBI Boston Field Office Press Release: FBI Warns of Teleconferencing and Online Classroom Hijacking During COVID-19 Pandemic.
2. Insider Higher Ed: 'Zoombombing' Attacks Disrupt Classes. Online Zoom classes were disrupted by individuals spewing racist, misogynistic or vulgar content. Experts say professors using Zoom should familiarize themselves with the program's settings.
3. New York Times: 'Zoombombing': When Video Conferences Go Wrong. As its user base rapidly expands, the videoconference app Zoom is seeing a rise in trolling and graphic content.
4. Forbes: Beware Zoom Users: Here's How People Can 'Zoom-Bomb' Your Chat
5. PCMag: How to Prevent Zoom-Bombing
6. Inc: 5 Ways to Protect Your Zoom Meetings From Hackers

If you have additional concerns or questions about Zoombombing, please reach out to us by submitting a request via the Minnesota State Service Desk at http://servicedesk.minnstate.edu/

Back to the top