

Best Practices for Securing Zoom Meetings

About this guide

This guide includes basic information and instructions on how to secure Zoom meetings before and during live sessions. Detailed instructions are available at the [Zoom Help Center](#), and additional information about teaching with Zoom is available through Concordia's [Centre for Teaching and Learning](#). Links to these resources are included throughout this document.

 **Note:** This guide recommends you disable certain features to ensure the security of your Zoom meetings. If you are interested in activities or teaching approaches that require you to enable these features, contact the Centre for Teaching and Learning at teaching@concordia.ca to discuss your options.

Important Recommendations

Before you get started with Zoom, please take note of the following recommendations:

- ✓ Never share your personal Zoom details on public forums, public webpages, or social media.
- ✓ Avoid using your Personal Meeting ID when you create public or virtual class meetings.
- ✓ Always use a different password for each meeting you schedule, including the recurring ones.
- ✓ Avoid posting pictures of private and virtual class meetings on social media or elsewhere online. Concordia University is committed to protecting the privacy of its community members and encourages faculty, staff, and students to avoid publicly posting images of private and virtual class meetings.

Getting Started

To get started, go to your Zoom profile in the [web portal](#) and check your default settings. These settings help secure your meetings, but you can enable and disable any of the options whenever you need to.

The following table includes the current default settings for all faculty and staff accounts.

| WHAT TO KEEP ENABLED | WHAT TO KEEP DISABLED |
|---|--|
| <p>Require a password when scheduling new meetings</p> <p>Use a different password for each new meeting to help secure every session.</p> | <p>Participants video</p> <p>Leave this option disabled so participants can decide when to turn on their video.</p> |
| <p>Mute participants upon entry</p> <p>Mute participants on entry to prevent unwanted clamour as everyone joins the meeting.</p> | <p>Join before host</p> <p>As the host, be the first to join the meeting so you can control who enters it. Avoid letting others join before you.</p> |
| <p>Prevent participants from saving chat</p> <p>For privacy reasons, <i>do not</i> allow participants to save the chats.</p> | <p>Use Personal Meeting ID (PMI) when scheduling a meeting</p> <p><i>Do not</i> use your PMI for public and virtual class meetings.</p> |
| <p>Screen sharing > Who can share? Host Only</p> <p>Enable Host Only to prevent uninvited screen sharing.</p> | <p>Embed password in invite link for one-click join</p> <p>Avoid using One-Click Join so only participants with the password can enter the meeting.</p> |
| <p>Waiting Room</p> <p>Use a waiting room so you can decide who joins your meeting and when.</p> | <p>File Transfer</p> <p>Prevent file transfer so participants cannot share potentially unsafe files.</p> |
| <p>Hide participant profile pictures in a meeting</p> <p>Leave this option enabled to prevent inappropriate images from being displayed.</p> | <p>Allow removed participants to rejoin</p> <p>Leave this option disabled to ensure removed participants cannot rejoin.</p> |

Scheduling a Secure Meeting

You can customize the settings for each of your meetings whenever you need to. But follow the guidelines in this section to ensure all your meetings are secure.

To schedule a secure meeting:

- ✓ **Use a random meeting ID:** Always generate a random meeting ID for your public and virtual class sessions. Doing so will reduce the likelihood that uninvited users can join your meetings. Random meeting IDs are the better alternative to using your **Personal Meeting ID (PMI)**. Your PMI is an ongoing meeting that anyone can join at any time once you have given them the ID number.
- ✓ **Password-protect your meetings:** Create a different password for each new meeting, including recurring ones. For staff meetings, you can share the password with your colleagues by email or calendar invite. For class meetings, you can share the password with students through Moodle so only those enrolled in the course can access the virtual classroom.
- ✓ **Require Registration:** If you enable this option, participants are asked to enter their email before they join the meeting. You can then see the email addresses of everyone who joined. This option is useful if you want to evaluate attendance.
- ✓ **Enable the Waiting Room:** Use the Waiting Room to admit invited participants and prevent uninvited or unknown users from entering the meeting.
- ✓ **Disable Join before host:** Make sure to disable this option so participants cannot join the meeting before you. For security purposes, the host should always be the first person to join a meeting. Anyone who tries to join before the host will receive a message that says, "The meeting is waiting for the host to join."

Securing a Meeting in Progress

Zoom comes with numerous security features that can help you communicate and teach effectively while preventing disruptions during your meetings.

To secure a meeting in progress:

- ✓ **Manage the Waiting Room:** When this feature is enabled, all participants are sent to a virtual waiting area. You can then admit them individually or all at once, keeping out any uninvited or unknown users.
- ✓ **Lock your meeting:** After your Zoom session has started, you can lock your meeting to prevent late or unexpected arrivals. Give participants a few minutes to join, and then lock the meeting.
- ✓ **Spotlight your video:** When three or more participants have their video turned on in a meeting, you can spotlight your video so everyone sees you as the active speaker. You can also spotlight the video of other participants as needed.
- ✓ **Control screen sharing:** By default, only hosts can share their screens during meetings. But you can change this setting before or during a session if you want to allow participants to share their screens. For class meetings, avoid giving All Participants the ability to share their screens. If a student needs to deliver a presentation, you can **enable or add a co-host** instead.
- ✓ **Lock the chat:** You can modify chat access to prevent participants from exchanging private messages during meetings. But avoid disabling the feature altogether. Allow participants to message you (the host) or communicate with the entire group through the chat as needed.
- ✓ **Mute participants:** With the recommended default settings, participants will be muted when they join the meeting. But you can also mute and unmute individual participants or all of them at once during the session.

- ✓ **Disable video:** You can turn off a participant's video to block distracting or inappropriate content during the session.
- ✓ **Disable participant annotation:** During class meetings, you can disable participant annotation in the screen sharing controls to prevent students from annotating your shared screen or whiteboard.
- ✓ **Remove a participant:** If an uninvited guest joins your meeting or if someone is being disruptive, you can remove the person from the Participants menu.
- ✓ **Attendee on-hold:** You can also temporarily disable a participant's audio and video connections by placing them on-hold.

Getting help

For detailed instructions and video tutorials, visit the [Zoom Help Center](#).

If you need help setting up your Zoom account or your meetings, contact the Service Desk at help@concordia.ca.

 **Note:** To ensure a safe and productive learning environment, teachers should carefully monitor students' use of screen sharing and annotation in breakout rooms. For more information about secure and effective teaching practices while using Zoom, visit Concordia University's [Centre for Teaching and Learning](#).

SOURCES

[Best Practices for Securing Your Virtual Classroom](#)

[Scheduling a Meeting](#)