Getting Started - Setting your Zoom Security Settings *Before* a meeting

This document walks you through all the Zoom security settings you can enable and disable PRIOR to hosting your Zoom meetings to ensure the most secure meeting possible.

Here's what's covered in this document (click on the menu item to advance to that section of the document):

Contents

If you have any questions after reviewing this document, or any other of our resources on the TLS Zoom at Carleton page, please email us at Zoom@carleton.ca

Top Security Recommendations

Follow these security recommendations regardless of the Zoom settings you enable or disable:

1. DON'T use your Personal Meeting ID (PMI) for public events. Your PMI is essentially one continuous meeting. Once people know the ID number, they can join the meeting at any time.

2. NEVER share your Zoom meeting links on publicly accessible forums. Instead, share link details through Brightspace so only enrolled students can access the virtual classroom.

3. NEVER use the same password for your Zoom meetings, even if you are scheduling a recurring meeting for a class. You can further protect your Zoom sessions by only sharing the password shortly before a class session.

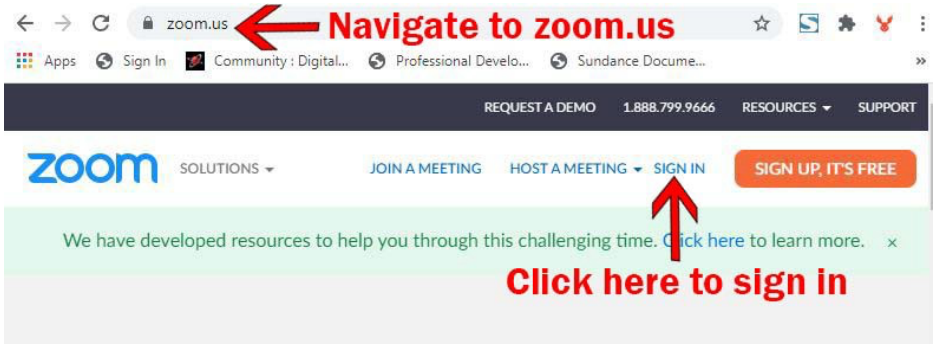
4. AVOID publicly posting images of private and virtual class meetings on social media or elsewhere online. This is important to protect the privacy of students, staff, and faculty.

5. DON'T share sensitive or confidential information on Zoom. As a standard practice, Zoom data mines all information provided on their service. There are reports that Zoom is capturing the browser 'tabs' that are open at the same time as Zoom. To avoid having Zoom gather this information, open Zoom in a private/incognito browser and avoid opening any additional tabs within that browser.

Enabling and Disabling Zoom Security Settings

Security settings are most comprehensive in the *Web version* of Zoom, so start by logging into your account online.

1. Navigate to https://zoom.us/
2. Click on the "Sign In" link in the top right corner



3. Click on "Settings" in the menu on the far left.
4. This will open a page with three tabs: Meeting, Recording, and Telephone. The chart below outlines what settings should be enabled and/or disabled in each tab.

Menu Tab	Left Menu Option	Option	Enable or Disable?
Meeting	Security	**Waiting Room** Use a waiting room so you can decide who joins your meeting and when.	Enable
		Require a passcode when scheduling new meetings Use a different password for each new meeting to help secure every session.	Enable
		Require a passcode for instant meetings A random passcode will be generated when starting an instant meeting.	Enable
		Require a passcode for Personal Meeting ID (PMI) Select "All meetings using PMI". NOTE: *do NOT* use your PMI for public and virtual class meetings.	Enable
		Embed passcode in invite link for one-click join Avoid using One-Click Join so only participants with the password can enter the meeting.	Disable
		Require passcode for participants joining by phone Passwords for all meetings is the best practice for keeping meetings secure.	Enable

Zoom Security Settings Continued

Menu Tab	Left Menu Option	Option	Enable or Disable?
Meeting	Security	**Only authenticated users can join meetings** This feature should not be used even though it would certainly increase security. The problem is that, if this feature is enabled, only students with a Zoom account will be able to join classes. Not all students will know to register for a free Zoom account in advance, which will present a barrier to them attending.	Disable (for now)
Meetings	Schedule Meeting	**Participants video** Leave this option disabled so participants can decide when to turn on their video. This will ensure student privacy is protected.	Disable
		Join before host As the host, be the first to join the meeting so you can control who enters it. Avoid letting others join before you.	Disable
		Use Personal Meeting ID (PMI) when scheduling a meeting Do NOT use your PMI for public and virtual class meetings.	Disable
		Mute participants upon entry This feature automatically mutes all participants when they join the meeting. In-meeting controls will allow you to enable participants to mute/unmute their mics.	Enable
Meetings	In Meeting (Basic)	**Require encryption for 3rd party endpoints (SIP/H.323)** This setting encrypts all 3rd party endpoints. Enable this setting just in case any one or any connection is using a SIP or H.323 system.	Enable
		Prevent participants from saving chat For privacy reasons, do NOT allow participants to save the chats.	Enable
		Private Chat This feature can be enabled if you want to allow students to be able to message each other privately without your knowledge. If you prefer that the chat only be used for public class discourse, disable this feature.	Either
		File Transfer Prevent file transfer so participants cannot share potentially unsafe files. This setting is automatically turned off, and you can turn it on if needed, but it is best practice to keep this setting disabled and only share documents through Brightspace.	Disable

Zoom Security Settings Continued

Menu Tab	Left Menu Option	Option	Enable or Disable?
Meetings	In Meeting (Basic)	**Screen Sharing> Who can share? Host Only** Enable Host Only to prevent uninvited screen sharing. If, during your class, you would like a student to share their screen, you can grant that access during the session.	Enable
		Annotation This feature can be enabled if you want to allow students to be able to use annotation tools to add information to shared screens. However, it might be best to keep this feature disabled.	Either
		WhiteBoard This feature can be enabled if you want to allow students to share a whiteboard during a session. This is most useful for breakout rooms. However, it might be best to keep this feature disabled.	Either
		Remote Control Turn this feature off to prevent others from being able to control the content you are sharing.	Disable
		Allow removed participants to rejoin Leave this option disabled to ensure removed participants cannot rejoin.	Disable
		Hide participant profile pictures in a meeting Leave this option enabled to prevent inappropriate images from being displayed.	Enable
Meetings	In Meeting (Advanced)	**Far end camera control** Allow another user to take control of your camera during a meeting. Both users (the one requesting control and the one giving control) must have this option turned on.	Disable
		Video filters Keep this option off to prevent users from apply filters to their videos, which can be distracting during class.	Disable
		Show a "Join from your browser" link Allow participants to bypass the Zoom application download process and join a meeting directly from their browser. This is a workaround for participants who are unable to download, install, or run applications and is important to keep enabled to ensure accessibility to the Zoom platform.	Enable
		Allow live streaming meetings Keep this option disabled to ensure meetings remain private.	Disable
Meetings	Other	**Blur snapshot on iOS task switcher** Enable this option to hide potentially sensitive information from the snapshot of the Zoom main window.	Enable

Zoom Security Settings Continued

Menu Tab	Left Menu Option	Option	Enable or Disable?
Recording*		**Advanced Cloud Recording Settings** Uncheck the "Display participants' names in the recording'" box to maintain participants' privacy. *Note: Due to extremely limited cloud recording space, we recommend you do record any Zoom meetings locally.*	Disable
		Require password to access shared cloud recordings Make sure a password is required to access any cloud recordings you share with others. *Note: Due to extremely limited cloud recording space, we recommend you do record any Zoom meetings locally.*	Enable
		Recording disclaimer For best practices, you should announce to students that you are recording a session *prior* to recording anything. This is made easy by enabling this feature.	Enable
		Multiple audio notifications of recorded meeting This feature ensures that anyone joining your session late will know that the session is being recorded.	Enable
Telephone		**Mask phone number in the participant list** Enable this feature to protect the privacy of students calling into a Zoom session by telephone.	Enable

***A brief note on recording Zoom sessions:**
Instructors may choose to record synchronous remote class sessions but must follow these guidelines set out by Carleton University.

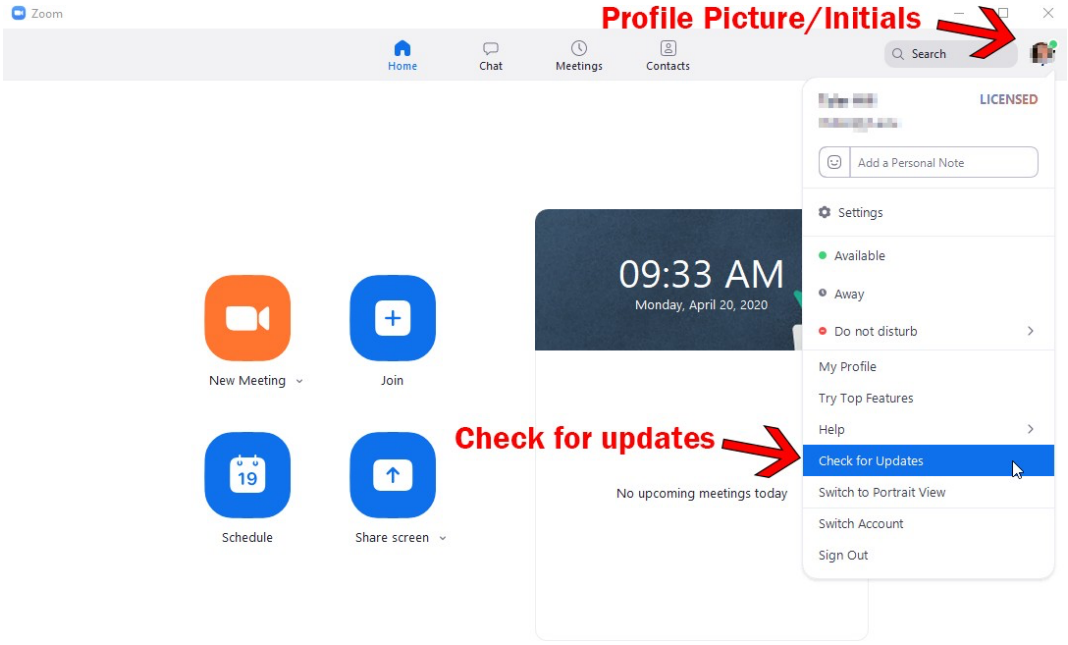
Students are prohibited from recording class sessions and are also prohibited from the distribution of class recordings.

Updating to the latest version of Zoom

One of the best ways to protect your Zoom sessions is to ensure you are using the latest version of Zoom. Since Zoom updates their system regularly, it's best to check your Zoom version every week or every two weeks. This is only applicable if you use the Desktop or Mobile Zoom applications.

Updating your Zoom Desktop Application

1. Open your Zoom desktop client.
2. Click on your profile picture (or initials if you do not have a profile picture set).
3. Select Check for Updates.



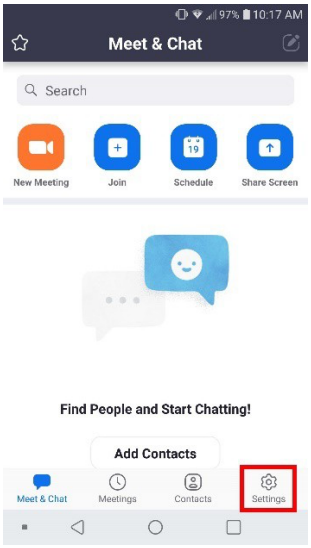
   a. If your desktop client is up to date, no further action is needed.
   b. If your client is out of date, you will be able to download and install the most recent version from here.
   c. You can also view the most recent release notes by clicking on the Release Notes hyperlink.

4. The latest Zoom desktop client can also be downloaded by visiting the Zoom Download Center. Be sure to download the option that is titled "Zoom Client for Meetings".

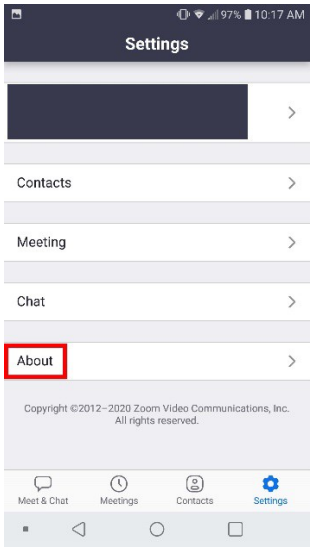
Updating your Zoom Mobile Application

Follow the instructions below to update your Zoom app on your mobile device.

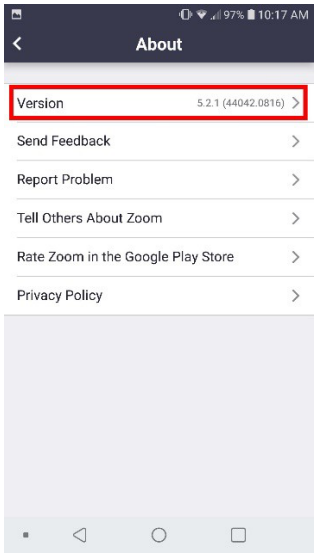
1. Open Zoom on your mobile device and in the bottom right-hand corner, click on the "Gear" symbol to access your settings.



2. Once in the settings menu, click on "About".



3. In the "About menu", you can click on the Zoom version, which will prompt your device to check for updates.



4. Your phone will either update your Zoom app to the latest version, or let you know the latest version is currently installed.