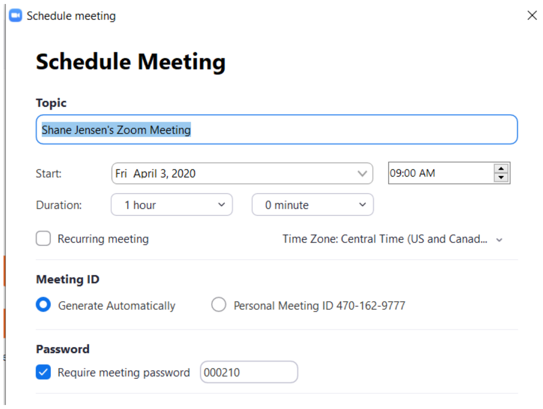
Tips for Securing Zoom…

Use your Minnstate Zoom account. Do not use a personal account for work purposes.

Add a password to your meetings

When creating a new Zoom meeting, Zoom will automatically enable the "Require meeting password" setting and assign a random 6 digit password.



Schedule meeting

Schedule Meeting

Topic: Shane Jensen's Zoom Meeting

Start: Fri April 3, 2020 09:00 AM

Duration: 1 hour 0 minute

☐ Recurring meeting Time Zone: Central Time (US and Canad...

Meeting ID

● Generate Automatically ○ Personal Meeting ID 470-162-9777

Password

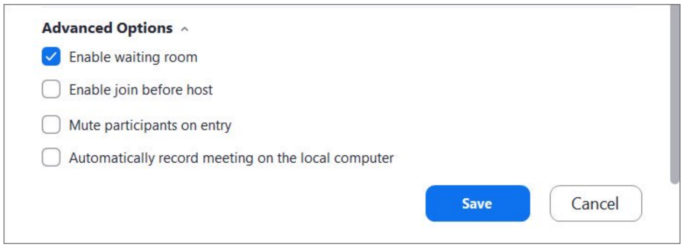
☑ Require meeting password 000210

You should not uncheck this option as doing so will allow anyone to gain access to your meeting without your permission.

Use waiting rooms

Zoom allows the host (the one who created the meeting) to enable a waiting room feature that prevents users from entering the meeting without first being admitted by the host.

This feature is now enabled by default during the meeting creation for all Minnstate meetings for all 'Guest' attendees.



Advanced Options

☑ Enable waiting room

☐ Enable join before host

☐ Mute participants on entry

☐ Automatically record meeting on the local computer

Enable waiting room setting

Anyone who joins the meeting, as a Guest, will be placed into a waiting room where they will be shown a message stating "Please wait, the meeting host will let you in soon."

The meeting host will then be alerted when anyone joins the meeting and can see those waiting by clicking on the 'Manage Participants' button on the meeting toolbar.

You can then hover your mouse over each waiting user and 'Admit' them if they belong in the meeting.

Tips for Securing Zoom…

Use your Minnstate Zoom account. Do not use a personal account for work purposes.

Keep Zoom client updated

If you are prompted to update your Zoom client, please install the update.

The latest Zoom updates enable Meeting passwords by default and add protection from people scanning for meeting IDs. The current version as of 4-3-20 is 4.6.9 (click your profile picture/icon in the top right, then 'check for updates')

With Zoom being so popular at this time, more threat actors will also focus on it to find vulnerabilities. By installing the latest updates as they are released, you will be protected from any discovered vulnerabilities.

Do not share your personal meeting ID

Each Zoom user is given a permanent 'Personal Meeting ID' (PMI) that is associated with their account.

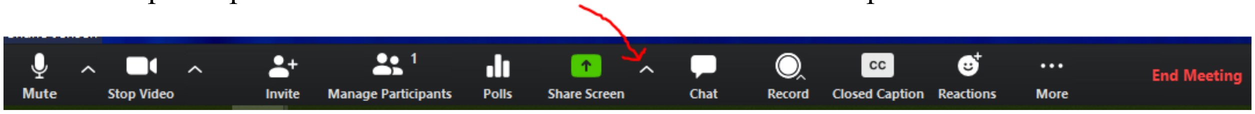
If you give your PMI to someone else, they will always be able to check if there is a meeting in progress and potentially join it if a password is not configured.

Instead of sharing your PMI, create new meetings each time that you will share with participants as necessary.

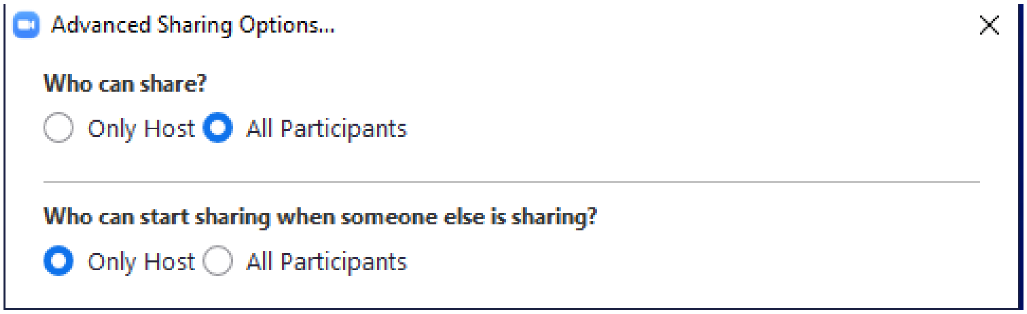
Disable participant screen sharing

To prevent your meeting from being hijacked by others, you should prevent participants other than the Host from sharing their screen. This is now the default setting for all Minnstate meetings.

To allow a participant to share their screen click the Share Screen up arrow as shown:



When the Advanced Sharing Options screen opens, change the 'Who Can Share?' setting to 'All Participants'.



Advanced Sharing Options...

Who can share?

○ Only Host ● All Participants

Who can start sharing when someone else is sharing?

● Only Host ○ All Participants

You can then close the settings screen by clicking on the X.

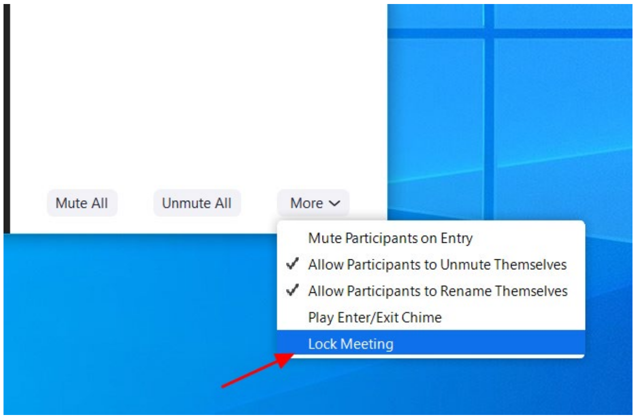
Tips for Securing Zoom…

Use your Minnstate Zoom account. Do not use a personal account for work purposes.

Lock meetings when everyone has joined

If everyone has joined your meeting and you are not inviting anyone else, you can Lock the meeting so that nobody else can join.

To do this, click on the 'Manage Participants' button on the Zoom toolbar and select 'More' at the bottom of the Participants pane. Then select the 'Lock Meeting' option as shown below.


Mute All
Unmute All
More
Mute Participants on Entry
✓ Allow Participants to Unmute Themselves
✓ Allow Participants to Rename Themselves
Play Enter/Exit Chime
Lock Meeting

Do not post pictures of your Zoom meetings

If you take a picture of your Zoom meeting, anyone who sees this picture will be able to see its associated meeting ID. This can then be used if uninvited people to try and access the meeting.

Do not share private data when you share your screen.

Worth saying twice: Do not share private date when you share your screen!

Tips for Securing Zoom…

Use your Minnstate Zoom account. Do not use a personal account for work purposes.

Do not post public links to your meetings

When creating Zoom meetings, you should never publicly post a link to your meeting (like Facebook, a web site, etc). Posting a link in D2L is fine.

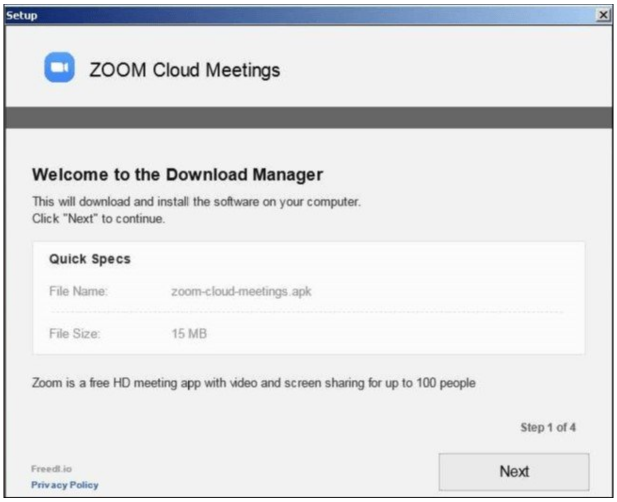
Doing so will cause search engines such as Google to index the links and make them accessible to anyone who searches for them.

As the default setting in Zoom is to embed passwords in the invite links, once a person has your Zoom link they can Zoom-bomb your meeting.

Be on the lookout for Zoom-themed malware

Since the Coronavirus outbreak, there has been a rapid increase in the number of threat actors creating malware, phishing scams, and other attacks related to the pandemic.

This includes malware and adware installers being created that pretend to be Zoom client installers.



Welcome to the Download Manager

This will download and install the software on your computer.
Click "Next" to continue.

Quick Specs

File Name: zoom-cloud-meetings.apk

File Size: 15 MB

Zoom is a free HD meeting app with video and screen sharing for up to 100 people

Malicious Zoom installer

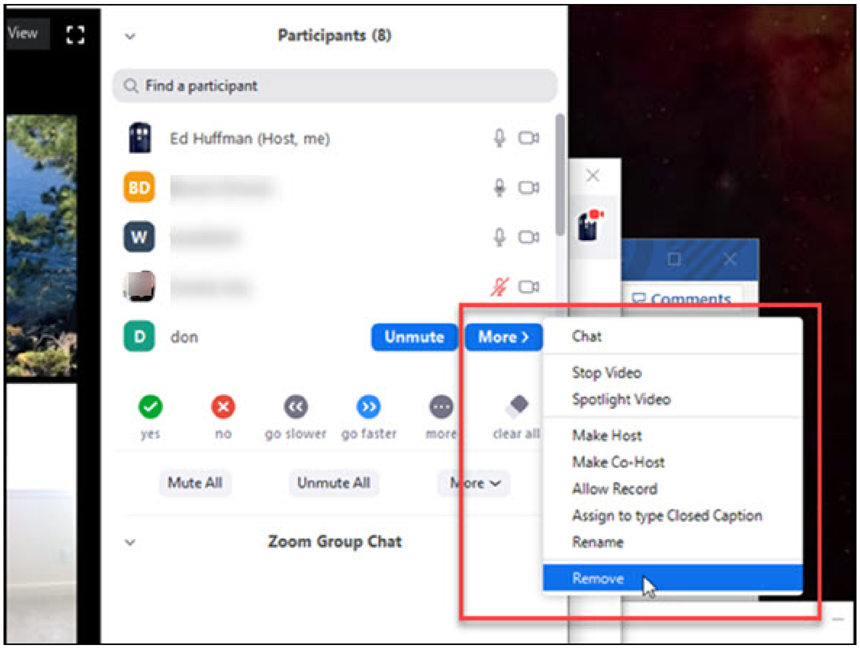
To be safe, only download the Zoom client directly from the legitimate Zoom.us site and not from anywhere else.

Tips for Securing Zoom…

Use your Minnstate Zoom account. Do not use a personal account for work purposes.

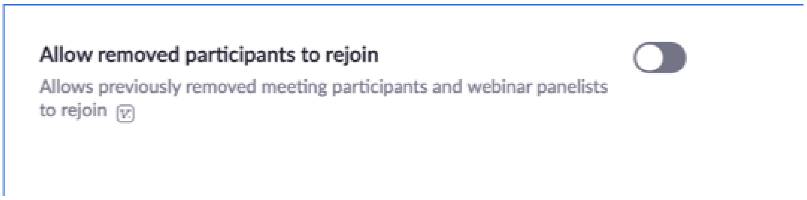
Remove a participant

As the host, you can remove a participant from a meeting in the participants panel



Zoom Participant list

And, if you turn off this option in your Zoom meeting **settings online**, they won't be able to rejoin.



Allow removed participants to rejoin

Allows previously removed meeting participants and webinar panelists to rejoin