Advisory-Zoom use for meetings, trainings etc.

Use of online meeting platforms like Zoom and Cisco Webex etc have seen a tremendous jump in conducting conferences, remote meetings and imparting education in the wake of COVID-19 lockdown across the world. Most of the users of these platforms are not aware of the correct way to configure these platforms to ensure security.

2. Recently various vulnerabilities and weaknesses have been reported in one of the most popular platform zoom. In present scenario, it may not be possible for all the sectors to stop using Zoom. Therefore, a comprehensive, graphical configuration setting has been prepared by CyCord Center for secure use of the platform.

3. Broad objective of enabling/disabling these settings is to

- prevent unauthorised entry in the conference room
- prevent an authorised participant to carry out malicious activities on the terminals of others in the conference.
- Avoid DOS attack by restricting users through passwords and access grant.

4. Most of the settings can be done by logging into users zoom account at website, or installed application at PC/Laptop/Phone and also during conduct of conference. However certain settings are possible through certain mode/channel only. For example *lock meeting* can be enabled by administrator only when the meeting has started. This documents explains in details all the security configuration through website, App and through console during the conference.

Objective of security configurations:

1. **Setting new user ID and password for each meeting**
2. **Enabling** *waiting Room,* so that every user can enter only when host conducting meeting admits him
3. **Disabling** *join before host*
4. Allowing **Screen Sharing by host Only**
5. Disabling **"Allow removed participants to re-join"**
6. **Restricting/disabling** *file transfer* option (if not required)
7. *Locking meeting*, once all attendees have joined
8. Restricting the recording feature
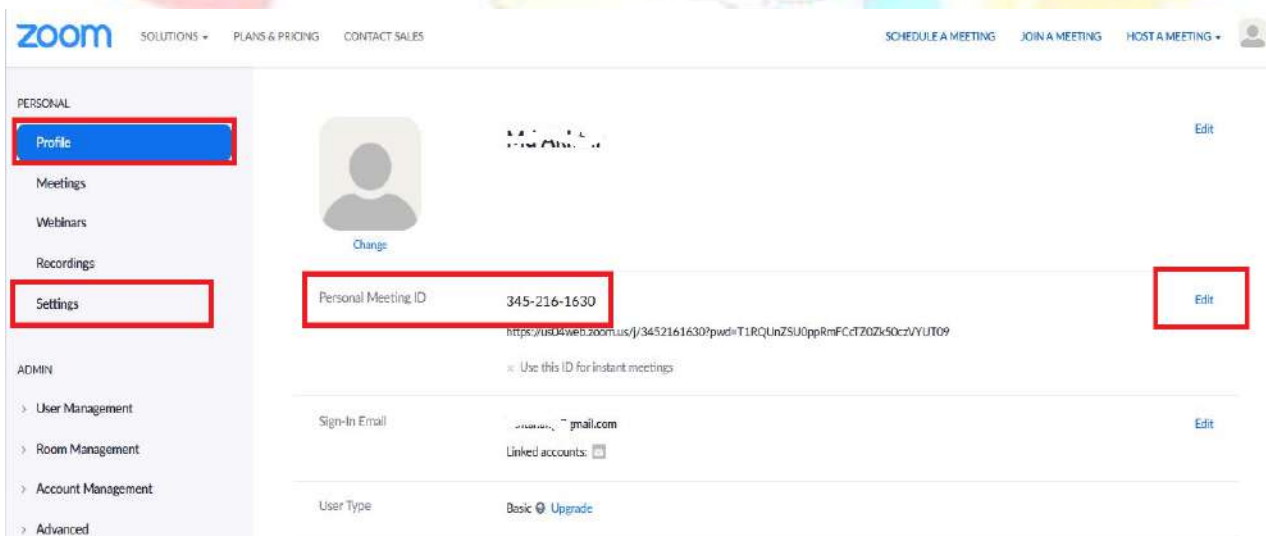9. To end meeting (and not just leave, if you are administrator)

Section 1: Security Configuration Through website

1. Logging into zoom Website: https://zoom.us/ by entering your account credentials

2. After login, page looks like this. Three important and useful links are shown in red boxes, profile, setting and personal meeting ID

3. Click profile-> edit button in front of personal meeting ID shown in above diagram and un-check the box shown below and click save changes.

Personal Meeting ID

345-216-1630

Only paid user can choose a Personal Meeting ID. Upgrade

Un-check ➡ ☐ Use Personal Meeting ID for instant meetings

Click save ➡ Save Changes   Cancel

4. Click the setting on home page and keep on scrolling down the window and make necessary configuration as shown in figures below. Only important ones are marked in red boxes and others could be anything

PERSONAL

Profile

Click here

Meetings

Webinars

Recordings

Settings

ADMIN

Meeting   Recording   Telephone

Schedule Meeting

In Meeting (Basic)

In Meeting (Advanced)

Email Notification

Other

Schedule Meeting

Host video
Start meetings with host

Participants video
Start meetings with parti
meeting.

Audio Type

Determine how participants can join the audio portion of the meeting. When joining audio, you can let them choose to use their computer microphone/speaker or use a telephone. You can also limit them to just one of those audio types. If you have 3rd party audio enabled, you can require that all participants follow the instructions you provide for using non-Zoom audio.

○ Telephone and Computer Audio

○ Telephone

◉ **Computer Audio**

Join before host

Allow participants to join the meeting before the host arrives

Use Personal Meeting ID (PMI) when scheduling a meeting

You can visit Personal Meeting Room to change your Personal Meeting settings.

Use Personal Meeting ID (PMI) when starting an instant meeting

Only authenticated users can join meetings from Web client

The participants need to authenticate prior to joining meetings from web client

Require a password when scheduling new meetings

A password will be generated when scheduling a meeting and participants require the password to join the meeting. The Personal Meeting ID (PMI) meetings are not included.

Require a password for instant meetings

A random password will be generated when starting an instant meeting

Require a password for Personal Meeting ID (PMI)

○ Only meetings with Join Before Host enabled

◉ All meetings using PMI

Password 0101 ✏

Embed password in meeting link for one-click join

Meeting password will be encrypted and included in the join meeting link to allow participants to join with just one click without having to enter the

Require password for participants joining by phone

A numeric password will be required for participants joining by phone if your meeting has a password. For meeting with an alphanumeric password, a numeric version will be generated.

Mute participants upon entry

Automatically mute all participants when they join the meeting. The host controls whether participants can unmute themselves. 🔽

In Meeting (Basic)

Require Encryption for 3rd Party Endpoints (H323/SIP)

Zoom requires encryption for all data between the Zoom cloud, Zoom client, and Zoom Room. Require encryption for 3rd party endpoints (H323/SIP).

Chat

Allow meeting participants to send a message visible to all participants

☑ Prevent participants from saving chat 🔽

Private chat

Allow meeting participants to send a private 1:1 message to another participant.

Auto saving chats

Automatically save all in-meeting chats so that hosts do not need to manually save the text of the chat after the meeting starts.

File transfer

Disable if not required

Hosts and participants can send files through the in-meeting chat. 🔽

Screen sharing

Allow host and participants to share their screen or content during meetings

Who can share?

◉ Host Only   ○ All Participants ⑦

Who can start sharing when someone else is sharing?

◉ Host Only   ○ All Participants ⑦

Disable desktop/screen share for users

Disable desktop or screen share in a meeting and only allow sharing of selected applications. 🗹

Annotation

Allow participants to use annotation tools to add information to shared screens 🗹

Whiteboard

if not required

Allow participants to share whiteboard during a meeting 🗹

Allow removed participants to rejoin

Allows previously removed meeting participants and webinar panelists to rejoin 🗹

Allow participants to rename themselves

Allow meeting participants and webinar panelists to rename themselves. 🗹

CyCord
One stop shop on all Cyber matters

Cyber Coordination Centre
Government of India

MINISTRY OF
HOME AFFAIRS
Government of India

Far end camera control

Allow another user to take control of your camera during a meeting

Virtual background

Allow users to replace their background with any selected image. Choose or upload an image in the Zoom Desktop application settings.

Identify guest participants in the meeting/webinar

Participants who belong to your account can see that a guest (someone who does not belong to your account) is participating in the meeting/webinar. The Participants list indicates which attendees are guests. The guests themselves do not see that they are listed as guests. [v]

Waiting room

Attendees cannot join a meeting until a host admits them individually from the waiting room. If Waiting room is enabled, the option for attendees to join the meeting before the host arrives is automatically disabled. [v]

Disable if not required

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. Note that the meeting experience from the browser is limited

Section 2: Security Configuration Through App
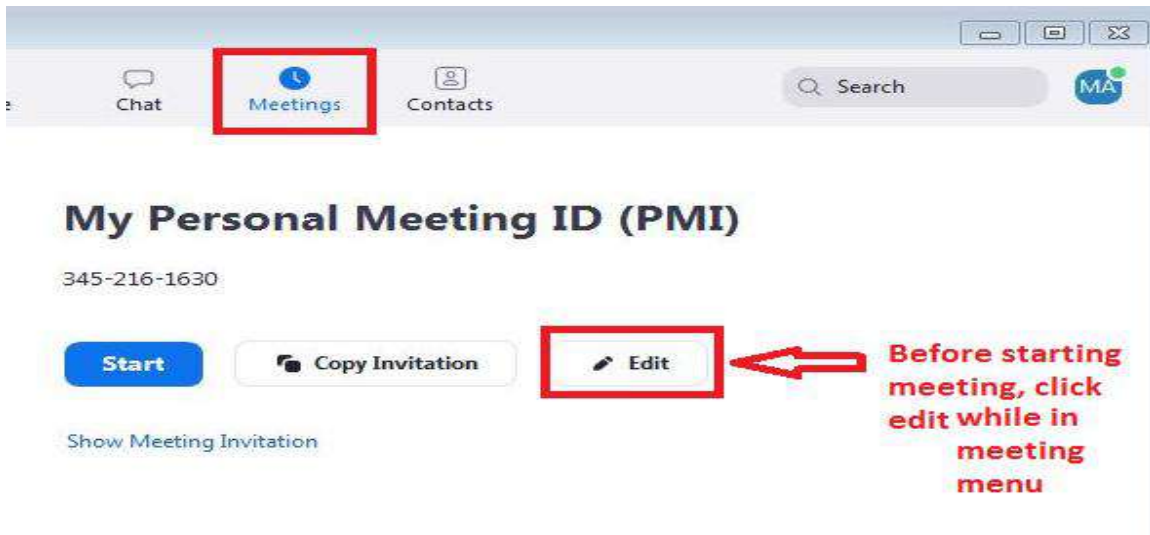
1. Zoom meeting App when launched look like this:
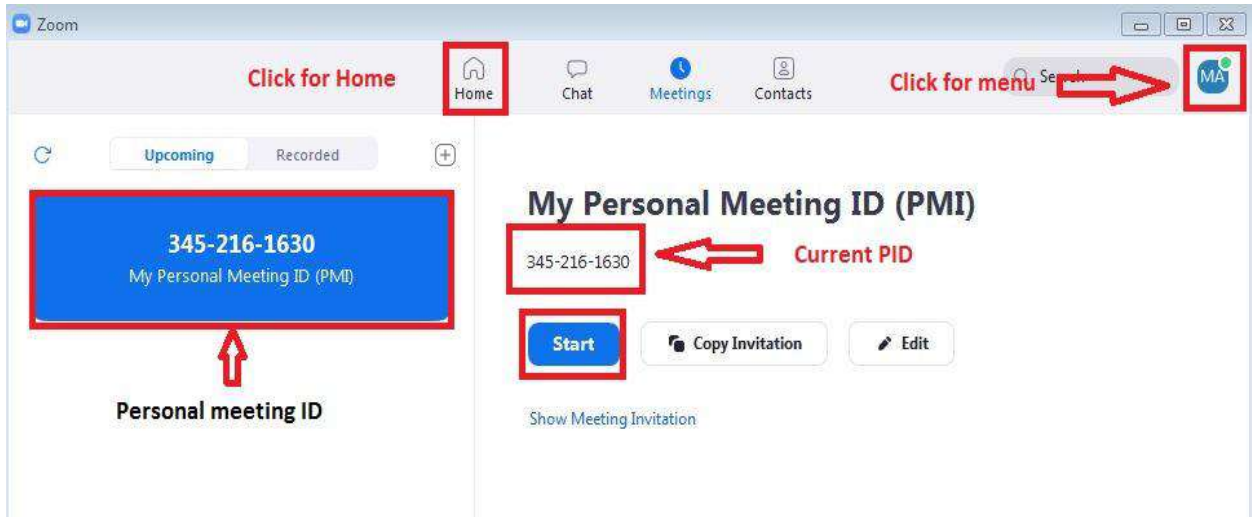
2. **Update your App:** First and fore most important thing is to update your Zoom App:

- click menu -> navigate to check for update -> click

CyCord
One stop shop on all Cyber matters

Cyber Coordination Centre
Government of India

MINISTRY OF
HOME AFFAIRS
Government of India
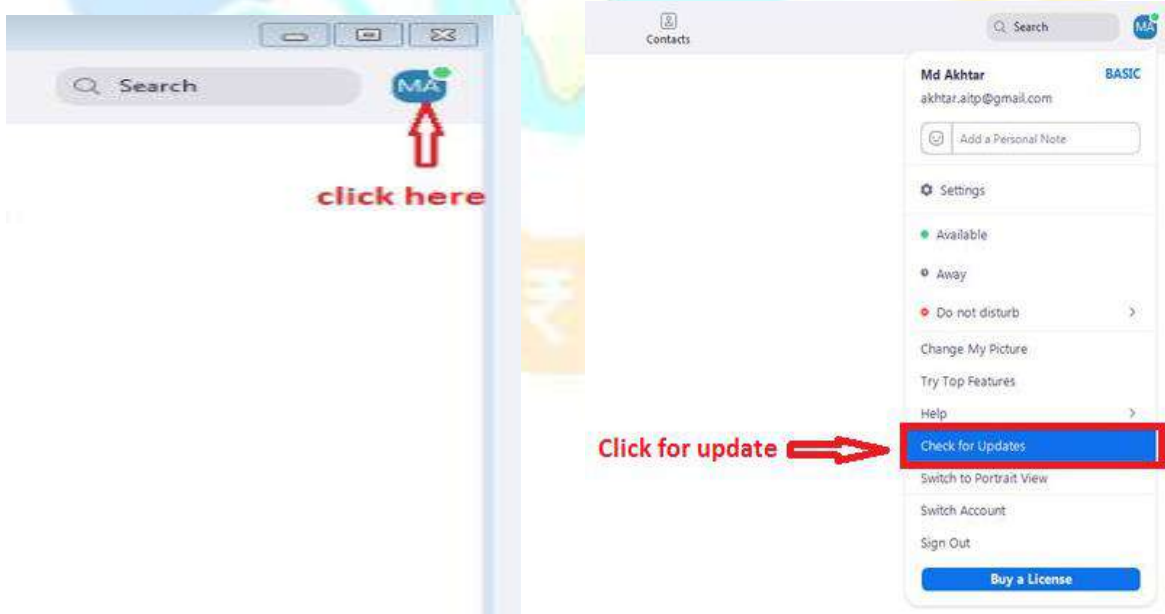
3. **Set a password** for personal meeting ID and **enable waiting**
- click edit in meeting as shown below

- Check password box, enter a strong password, check enable waiting window etc. desirable settings are shown in red boxes and click save

4. **Avoid** conducting meeting by using Personal Meeting ID (PMI).

Clicking on start as shown below will start a meeting with personal meeting ID and password set by user as shown above. In this case PMI: 3452161630 and password: Sc@3Q*
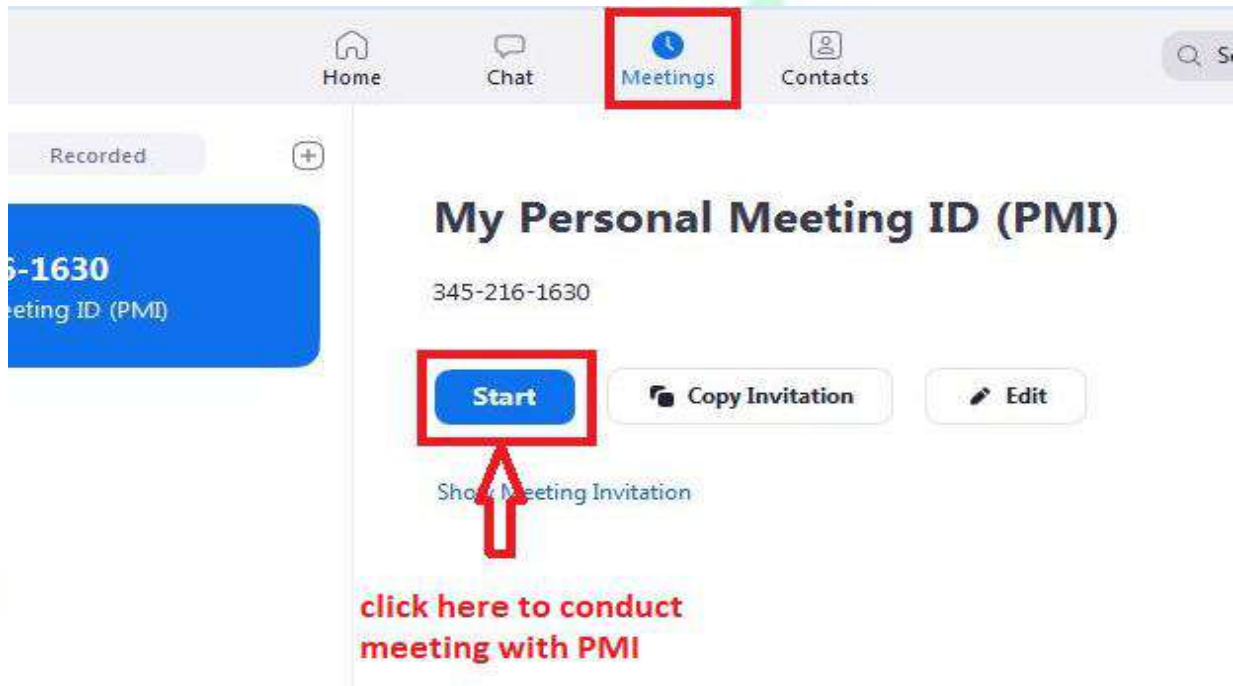
Problem in suing personal meeting ID is that with PMI and password is fixed. It does not automatically change with every new meeting.

5. **Conduct a new meeting with randomly generated ID and password** instead of fixed one as shown above
   • Click on home

CyCord
One stop shop on all Cyber matters

Cyber Coordination Centre
Government of India

MINISTRY OF
HOME AFFAIRS
Government of India
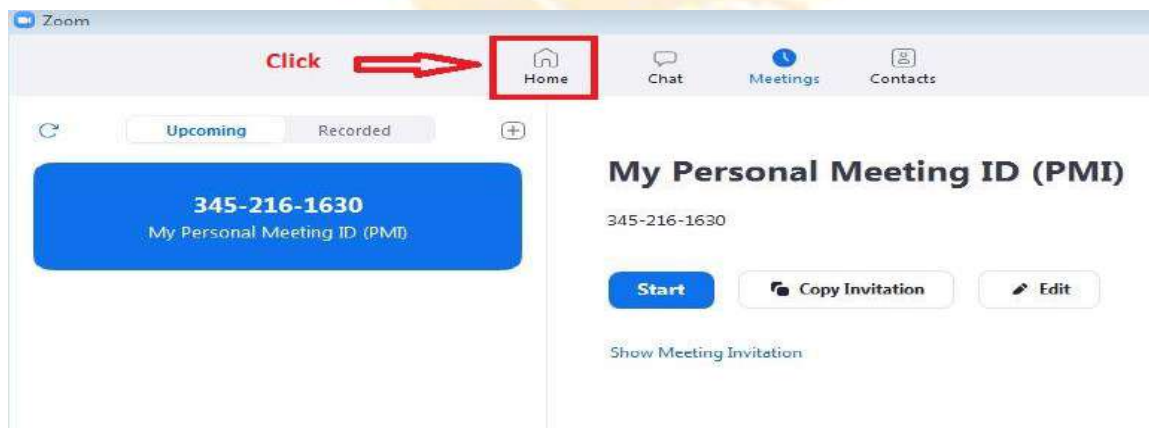
- Click New Meeting drop down as shown below
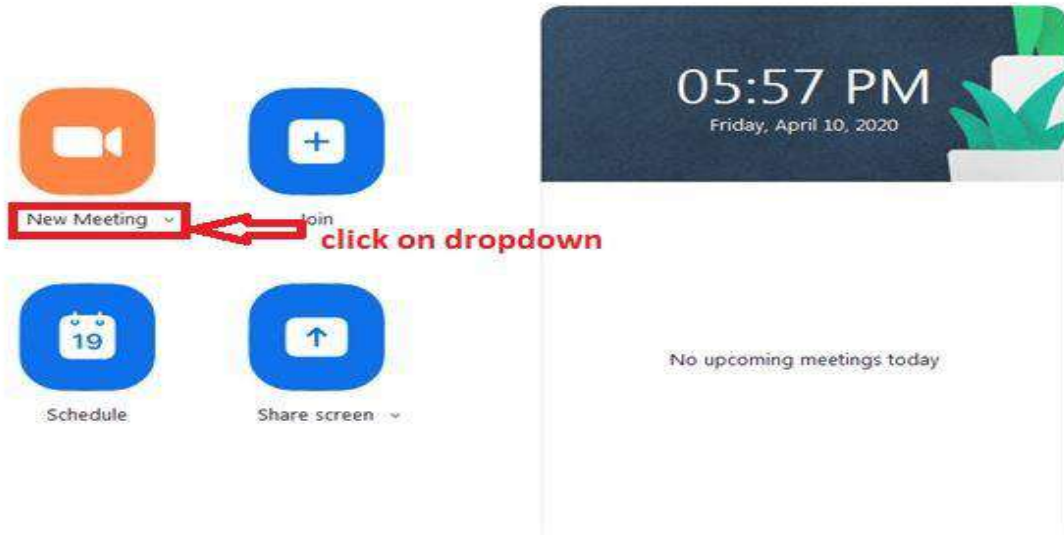
- Un-check use My Personal Meeting ID (PMI), if not already done
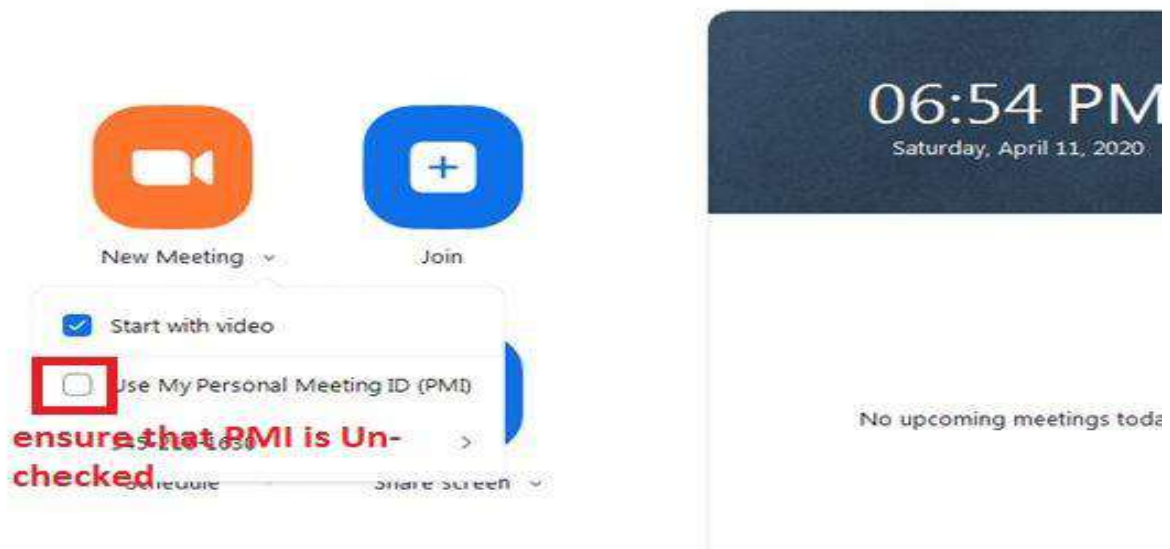
- Click new meeting icon to start a new meeting
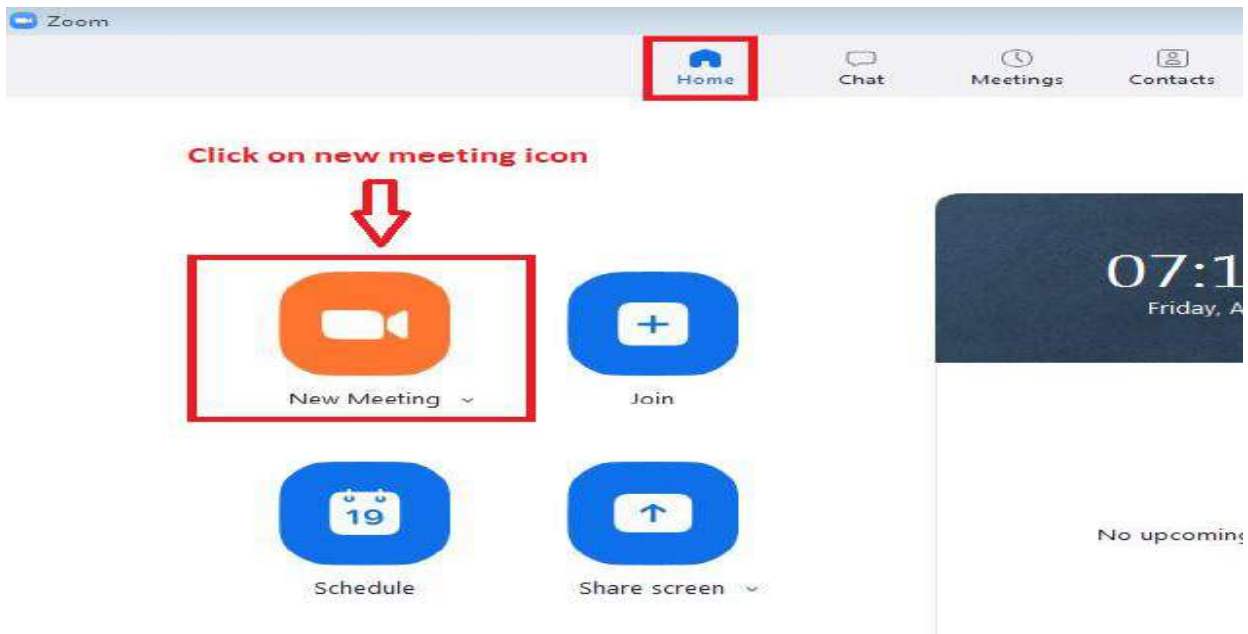
- Once Meeting has started, you will see your meeting ID and password by clicking left top icon below. it will be random and change with every new meeting.
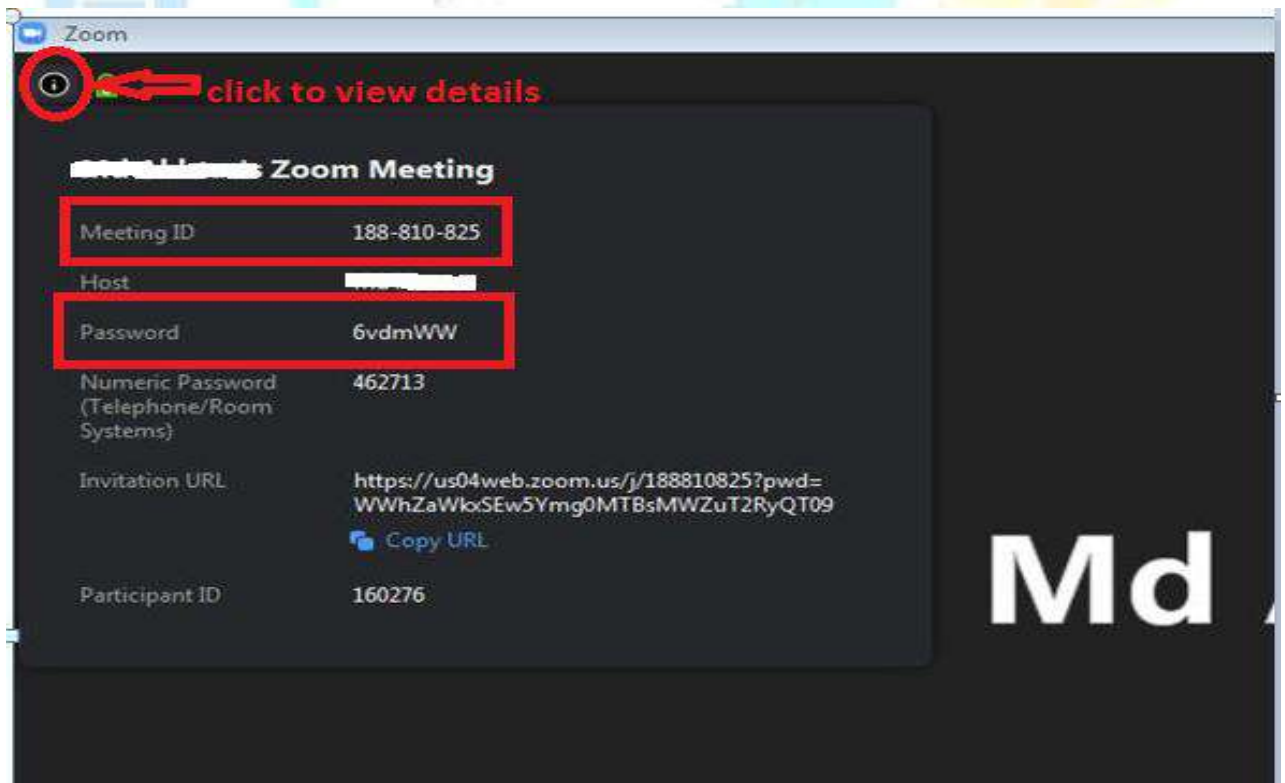
6. Scheduling a meeting with randomly generated ID and password
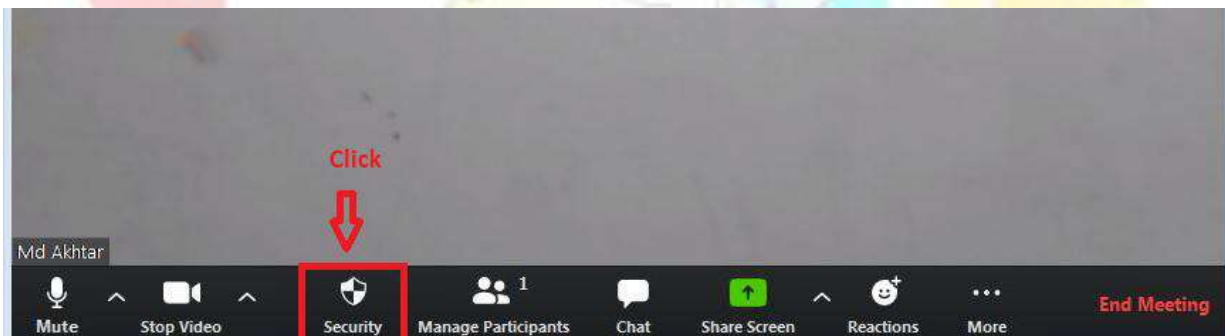
- Click schedule as shown below

- The window as shown below will open up

- After clicking *advanced Options* shown in above window following expansion will open and do setting as shown below.
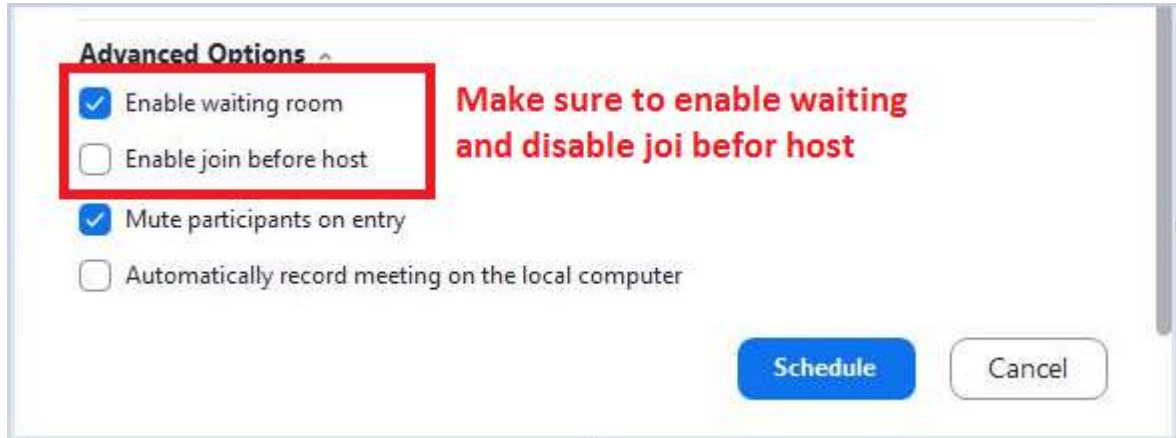
6. **Lock the meeting** session, once all attendees have joined

- Once meeting is in progress, control bar looks like this

- Click Security and click on Lock Meeting, if all your participants have joined. you can enable waiting room from here also. you can also disable share screen by users from here
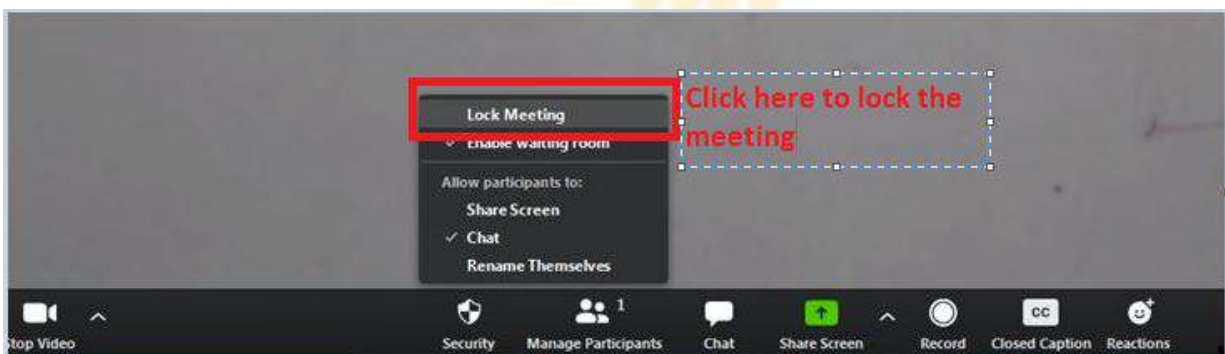
Miscellaneous tips:

- Don't use your personal meeting Id (PMI) to host event, instead use randomly generated meeting IDs for each event.
- Don't share your link on public platform, instead share randomly generated meeting id and password for every new meeting session/schedule. It makes it much secure and difficult to leak.
- If you are admin, remember to end meeting, dont just leave meeting.
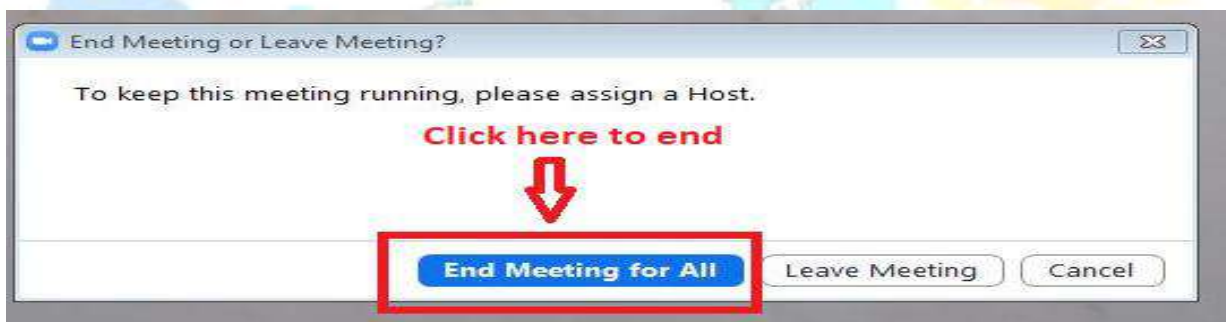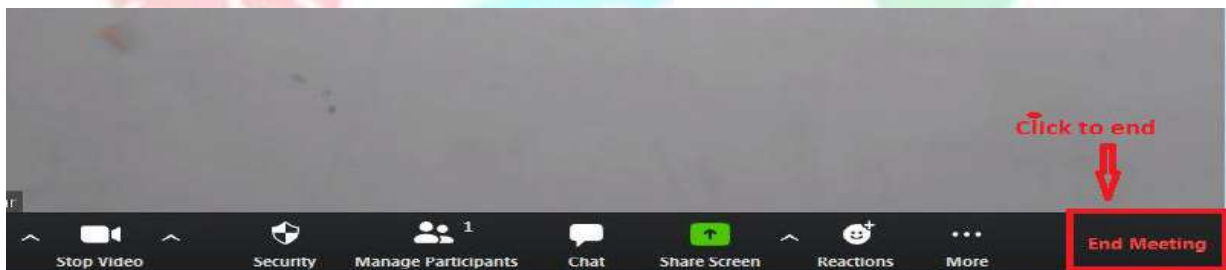
- Sign out of your account when not in use

****

Cycord Support Team
E-mail: cycordsupport.mha@gov.in
Land Line: 011- 26531614, 011-26510245
whatsapp: +917292045198
Website: www.cycord.gov.in