CMSGu2020-01

National Computer Board

Mauritian Computer Emergency Response Team

Enhancing Cyber Security in Mauritius

Guideline for schools and parents on cybersecurity and safety during the coronavirus lockdown

CERT-MU

National Computer Board

Mauritius

Version 1.0

April 2020

Issue No. 1

Table of Contents

1.0 Introduction.......................................5

1.1 Purpose and Scope.......................................5

1.2 Audience.......................................5

1.3 Document Structure.......................................5

2.0 Background.......................................6

3.0 Common video calling/conferencing apps used by students and teachers during lockdown.......................................7

3.1 Microsoft Teams.......................................7

3.2 Zoom.......................................8

3.3 Messenger.......................................8

3.4 WhatsApp.......................................9

3.5 Skype.......................................10

3.6 Google Duo.......................................10

3.0 Online abuse trend during the COVID-19 pandemic.......................................11

3.1 Online sexual exploitation and grooming.......................................11

3.2 Sexting.......................................11

3.3 Exposure to harmful/violent content.......................................11

3.4 Cyberbullying.......................................11

3.5 Increase in messaging, voice and video calling.......................................12

3.6 Exposure to and propagation of fake news/misinformation.......................................12

4.0 What can schools do to protect students?.......................................13

4.1 Not to engage with cyberbullies.......................................13

4.2 Never meet people in real life.......................................13

4.3 Monitor behavioural changes.......................................13

4.4 Not to get involved in identity theft 13

4.5 Not to forward fake news/misinformation 13

4.6 Courses and activities for students 14

4.7 Promote responsible use of technology and information 14

5.0 What can parents do to protect their children? 15

5.1. Establish house rules 15

5.2 Encourage your children to use the computer/laptop/tablet/mobile phone in open, shared spaces 15

5.3 Encourage and maintain an open an ongoing dialogue with your children 15

5.4 Encourage your children to think before they click 15

5.5 Always check for harmful content 16

5.6 Discuss the risks of posting and sharing private information 16

5.7 Be a good role model 16

5.8 Use a robust and trusted security software solution 16

6.0 Conclusion 17

Annex 1 Privacy and Security considerations when using Zoom 18

References 25

***DISCLAIMER:** This guideline is provided "as is" for informational purposes only. Information in this guideline, including references, is subject to change without notice. The products mentioned herein are the trademarks of their respective owners.*

1.0 Introduction

1.1 Purpose and Scope

The purpose of this guideline is to present to schools and parents the different threats that are on the rise during the lockdown as many children are engaging in online school work and assignments. The guideline also gives details on how to protect the children while they are surfing on the Internet.

1.2 Audience

The targeted audience for this document includes all headmasters, rectors, teachers and parents whose students and children have access to the Internet at home.

1.3 Document Structure

This document is organised into the following sections:

Section 1 gives an outline of the document’s content, the targeted audience and the document’s structure.

Section 2 gives a general background on children’s online exposure to online dangers during the lockdown.

Section 3 gives an overview on the online abuse trend during the COVID-19 pandemic.

Section 4 explains what measures schools can take to protect students.

Section 5 gives details on what parents can do at home to provide a safer online experience for their children.

Section 6 concludes the document.

2.0 Background

The coronavirus (COVID 19) pandemic has led to an unprecedented rise in screen time. School closures and strict containment measures mean more and more families are relying on technology and digital solutions to keep children learning, entertained and connected to the outside world. On the other hand, not all children have the necessary knowledge, skills and resources to keep themselves safe online. Not only countless children are shifting to the online world for the very first time, but they are also spending more time online during the lockdown.

In millions of homes over the world, parents are juggling like never before as they struggle to teach their children while working from home during the coronavirus lockdown. With their normal weekday routines gone, many children are finding it hard to suddenly have mum and dad as teachers, and many parents are trying to control the urge not to scream at them.

Moreover, for many children, the global lockdown has also meant going online earlier than may have been expected. The sudden swing to home schooling has meant that children, aged 9 and 11 have been given mobile phones earlier than planned, simply so that they can keep up to date with schoolwork, educational activities and friends in this difficult time.

Protecting children online during this worldwide health emergency is a global challenge, which requires a global approach. While many efforts to improve child online protection are already under way, their reach has been more national than global.

3.0 Common video calling/conferencing apps used by students and teachers during lockdown

Video conference has become the normal way to communicate during the lockdown. Even students are attending classes via video calling apps. Hence, the popularity of these apps has exploded in the last few weeks. Below are some of the video conferencing tools that is commonly used. Parents can follow the steps to get accustomed with them.

3.1 Microsoft Teams

Microsoft Teams is a unified communication and collaboration platform that combines persistent workplace chat, video meetings, file storage, and application integration. Microsoft teams for students is meant to engage students with virtual face-to-face connections and activities, or set up a remote lunch to keep classrooms connected and having fun and it is free for students and teachers with a valid school email address.

- To sign in in Windows, click **Start** > **Microsoft Teams**. On Mac, go to the **Applications** folder and click **Microsoft Teams**. On mobile, tap the **Teams** icon. Then sign in with your Microsoft 365 username and password. (If you're using Teams free, sign in with that username and password.)
- To pick a team and channel, select **Teams** and choose a team. Pick a channel to explore **Posts**, **Files**, and other tabs.
- To start a conversation with the whole team, select **Teams**, pick a team and channel, write your message, and click **Send.** To start a conversation with a person or group, click **New chat**, type the name of the person or group in the **To** field, write your message, and click **Send.**
- To make video and audio calls, click **Video call** or **Audio call** to call someone from a chat. To dial a number, click **Calls** on the left and enter a phone number. View your call history and voicemail in the same area.
- To reply to a post, find the thread you want to reply to, then click **Reply**. Add your thoughts and click **Send**.

- To share a file, click **Attach** under the box where you type messages, select the file location and then the file you want. Depending on the location of the file, you'll get options for uploading a copy, sharing a link, or other ways to share.
- To work with files, click **Files** on the left to see all files shared across all of your *teams*. Click **Files** at the top of a channel to see all files shared in that *channel*. Click **More options ...** next to a file to see what you can do with it.

3.2 Zoom

Zoom is basically a video conferencing app for virtual meetings and hangouts. It was previously limited to businesses but the lockdown across countries has brought Zoom to the mainstream, being used by thousands of people.

- Firstly, you need to download the Zoom application on your desktop or smartphone.
- Once you have successfully downloaded it, simply launch the app and choose between Join a Meeting option or Sign In.
- After you have signed up or logged into the platform by following the on-screen steps, go to the home screen and start the process of setting up a new meeting.

Many organisations have reported that there were privacy and security issues with Zoom. Therefore, it is advised that you follow the security tips provided in *Annex 1* of this guideline to secure your Zoom meeting.

3.3 Messenger

Facebook recently worked to streamline Messenger, the app has been separate from the main Facebook app for several years now. Messenger is used by many individuals and businesses for communication and you can even use it without a Facebook account.

You can do a video chat with just one person, or with a group of people. Steps you can follow to do a video call.

- To video chat with one person, you need to open a conversation with the person you want to video chat with and tap **Video Camera**
- To video chat with a group, you need to open a group conversation with the people you want to video chat with and tap **Video Camera**.
- If you are using a desktop app then open the conversation with the person or group you want to video chat and tap **Video Camera**.

3.4 WhatsApp

Facebook-owned WhatsApp is one of the massively used apps. As of early 2020, WhatsApp has over two billion users worldwide. WhatsApp is an easy to use app, all it's messages and call data are protected with end-to-end encryption which basically means that the data can only be read or accessed by the users in the conversation.

You can make new chats and search for messages in the past. You can also see when messages are received and read and it's just great with pictures. You can even use it for making a video call and voice calls. You can start a call with one individual and then add other participants easily.

- To place a video call you need to open the chat with the contact you want to video call and tap **Video Call.**
- To make a group video call from a group, you need to go to the group you want to video call. Tap New Call and select the contacts you want to add to the call and tap **Video Call**.

You can even make a group video call from the Calls tab. You first need to go to the Calls tab after that tap New Call > New Group Call. Next, you need to select the contacts you want to add to the call and tap Video Call.

You can even make a group video call from an individual chat. To do so you first need to open the chat with one of the contacts you want to video call and tap Video Call. Once the particular contact accepts the call, tap Add Participant, search for or select another contact and tap Add.

3.5 Skype

Skype is a telecommunications application that specializes in providing video chat and voice calls between computers, tablets, mobile devices. After global lockdowns were imposed, the usage in Skype's video calls increased by 70 percent, according to a report by Reuters. Below are the steps you can follow to make a call via Skype.

- To make a call you first need to find the person you want to call from your Contacts list. Next, you need to select that contact and tap the Video call icon.
- To make a group call, from your call list you need to select the new call option and then select all the participants you want to call and at last tap the video call icon.

3.6 Google Duo

Google Duo is a video chat mobile app produced by Google. You can use Google Duo to make video calls to your family, friends, and anyone else. Google Duo is a free service available for both Android and iOS devices. All your calls in Google Duo are encrypted, which means that they are private to you and the person you are calling.

Here are the steps you can follow to make a video call via Google Duo.

- Select the person you would like to call from your contacts or type in the number you'd like to reach. Next tap Video call.
- To create a group, select the Create Group icon and select up to 11 participants you want to do a group video call with.
- Once selected, click on Next, and then name the group. You can hit the Video Call button to start the video call.

3.0 Online abuse trend during the COVID-19 pandemic

More than 1.5 billion children and young people have been affected by school closures across the globe. Many of these students are now taking classes as well as socializing more online.

3.1 Online sexual exploitation and grooming

Spending more time on virtual platforms can leave children vulnerable to online sexual exploitation and grooming, as predators look to exploit the COVID-19 pandemic.

3.2 Sexting

your friends lol

i swear i won't show anyone

ever????

i promise

A lack of face-to-face contact with friends and partners may lead to heightened risk-taking such as sending sexualized images.

3.3 Exposure to harmful/violent content

Increased and free time online may expose children to potentially harmful and violent content.

3.4 Cyberbullying

There is also a greater risk of cyberbullying which comes along the way with children being confined and not being able to express themselves verbally.

3.5 Increase in messaging, voice and video calling

Facebook reports new usage records almost every day across all of its platforms. In many places messaging, voice and video calling have more than doubled on its Facebook Messenger and WhatsApp platforms.

3.6 Exposure to and propagation of fake news/misinformation

With mobile apps such as Whatsapp and social networking sites such as Facebook, it is more than easy to not only post, but also receive all kinds of information. Many of those information is fake and very often children are tempted to forward these to their friends, parents or relatives.

4.0 What can schools do to protect students?

Head of schools and teachers can work towards updating existing safeguarding policies or creating new ones to reflect the new realities for children learning from home; promote and monitor good online behaviours and ensure that children have continued access to school-based counselling services. The following can be used as guidelines to teach students to be safe online and identify any reaping issues:

4.1 Not to engage with cyberbullies

Students should be taught to not engage or argue with cyberbullies as it might encourage even worse behaviour. They should use the built-in filters to prevent further harassment through e-mail or instant messaging by cyberbullies.

4.2 Never meet people in real life

Students need to be explained that they should never meet people they have known only through online internet and should not do anything online which is not preferred to be done in the presence of others.

4.3 Monitor behavioural changes

Teachers should try and monitor students through video conferencing for behavioral changes and difference in their attitude.

4.4 Not to get involved in identity theft

Students should not log in as someone else to read their e-mails or mess with their online profiles; attempt to infect or in any way try to make someone else's computer unusable and not download any attachments from an unknown source as they may contain viruses.

4.5 Not to forward fake news/misinformation

Students should be taught not to propagate fake news and not also not to believe everything they see or receive on COVID-19. There should be a clear demarcation between facts and fake news. Students should also know that there are existing laws (Information and Communication Technologies Act) that cater for fake news in Mauritius.

4.6 Courses and activities for students

Schools can introduce courses and activities for students on major aspects of cyber security and safety.

4.7 Promote responsible use of technology and information

Schools should support, model and teach safe, legal, and ethical use of digital information and technology; promote and model responsible social interactions related to the use of technology and information; celebrate cyber security week and conduct activities to create awareness through cyber clubs.

5.0 What can parents do to protect their children?

Parents need to ensure their children's devices have the latest software updates and antivirus programs; have open dialogues with them on how and with whom they are communicating online; work with them to establish rules for how, when, and where the internet can be used; be alert to signs of distress in children that may emerge in connection with their online activity, and be familiar with school policies and local reporting mechanisms and have access to numbers of support helplines and hotline handy. Below is a set of guidelines that parents can follow to ensure a safer online experience for their children:

5.1. Establish house rules

These can include setting limits to screen time (e.g. 1 hour), the type of content a child accesses online through their mobiles and other devices (e.g. content meant for children according to their age) or the appropriate tone of language to use online. These rules should vary depending on your children's age, maturity and understanding of the risks they could face online.

5.2 Encourage your children to use the computer/laptop/tablet/mobile phone in open, shared spaces

This is about striking a balance where they do not feel that you are constantly looking over their shoulder and do not feel like they need to hide to go online. It will help put your mind at ease about what they are doing, and they will know they can come to you if they are confused, frightened or concerned.

5.3 Encourage and maintain an open an ongoing dialogue with your children

Talk to your children about mobile use and experiences online. Maintain an open conversation with them.

5.4 Encourage your children to think before they click

Whether they are looking at online video sites, receiving an unknown link in an email or even browsing the web, remind your children not to click on links which may take them to dangerous or inappropriate sites. Clicking unknown links is a common way people get viruses or reveal private and valuable information about themselves.

5.5 Always check for harmful content

From websites to mobile apps, games and online communities, your children have access to a lot of content that can affect them both positively and negatively. Using smart family security and parental control features, as well as the built-in security settings in your browsers, can help the whole family stay safe.

5.6 Discuss the risks of posting and sharing private information

Encourage your children to think about the videos, photographs and information they share through mobiles, especially on social media.

5.7 Be a good role model

Children are likely to imitate their parents' and other adult's behaviour, so as responsible parents we have to lead by example.

5.8 Use a robust and trusted security software solution

This can help create a safe online experience for children online by managing restricted sites access, browsing history preview and setting limits screen time.

In addition to the above, parents should be aware of what their children are watching or listening to on the internet. There are some websites that may pose a threat as they may try to entice children and persuade them to exchange personal information including phone numbers or address.

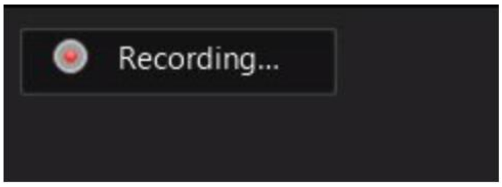
- There should be two-factor authentication for devices and its home screen should be locked with a pin.
- Teach children how to browse and the content that needs to be looked for in order to maintain appropriate online behaviour.
- Take your children seriously if he or she reports an uncomfortable online exchange.
- Teach your children that the internet provides anonymity. Therefore, someone they come in contact with may not be who they think they are.
- Keep a check on credit card and phone bills as well and look for unfamiliar account charges.

6.0 Conclusion

With schools closed and many parents and teachers working remotely, children are more likely to be using the internet unsupervised. Worryingly, abusers see this as an opportunity to target children who are spending more time online and may be feeling increasingly lonely or anxious because of the lockdown. Therefore, it is now more important than ever for schools and parents to be having regular conversations with their students and children about what they are doing online and giving them the assurance they can share any worries they may have at all times.

Annex 1 Privacy and Security considerations when using Zoom

Before starting to use Zoom, it is important to consider the privacy implications of participating in meetings. A Host (the one who created the meeting) can record a Zoom session, including the video and audio, to their computer. It is therefore advised to be vigilant before saying or revealing anything that you would not want anybody else to potentially see or know about. Participants will know when a meeting is being recorded as there will be a **Recording...** indicator displayed in the top left of the meeting as shown below:



Recording...

Figure 1: Recording

A user can download their chat logs before leaving a meeting. These logs will only contain messages that you could see, but not the private chat messages of other users.

Moreover, it has been reported that there is no true end-to-end encryption (E2E) between Zoom users' endpoints. This means that only the communication between a meeting participant and Zoom's servers is encrypted, while the related meeting data traversing over Zoom's network is not. This also means that a Zoom employee could monitor a meeting's traffic and spy over it. However, the vendor has stated that there are security settings in place to prevent this type of activity

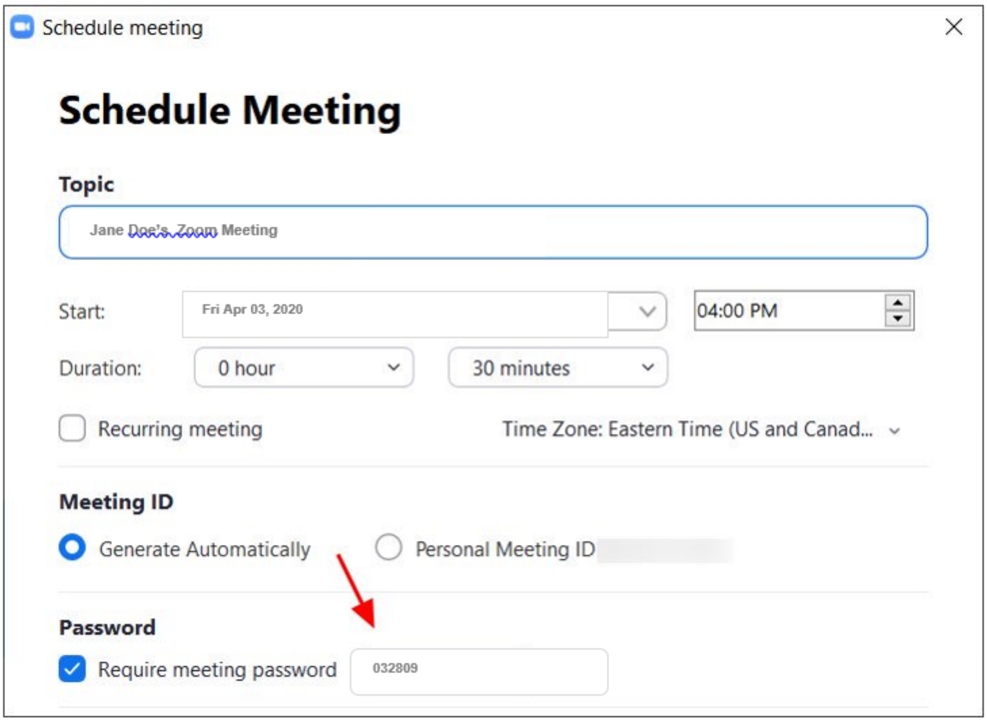
Zoom Security Tips

1. **Always download the latest version of the Zoom application from the official website**

   To avoid fake and malicious software, it is recommended to download the latest available application from the official Zoom website (www.zoom.us).

2. **Use a password for all 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

Jane Doe's Zoom Meeting

Start: Fri Apr 03, 2020 04:00 PM

Duration: 0 hour 30 minutes

□ Recurring meeting Time Zone: Eastern Time (US and Canad...

Meeting ID

● Generate Automatically ○ Personal Meeting ID

Password

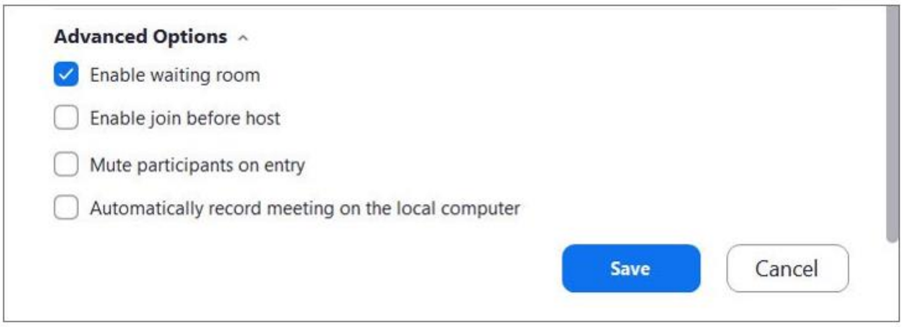
☑ Require meeting password 032809

Figure 2: Schedule Meeting

This option should always be checked as this will prevent unauthorized access to your meeting.

3. Make Use of Waiting Room

Zoom allows the host (the one who initiated the meeting) to enable a waiting room feature that prevents users from entering the meeting without first being admitted by the host. This feature can be enabled during the meeting creation by opening the advanced settings, checking the **Enable waiting room** setting, and then clicking on the **Save** button.



Advanced Options

☑ Enable waiting room

□ Enable join before host

□ Mute participants on entry

□ Automatically record meeting on the local computer

Figure 3: Waiting Room Option Setting

When the **waiting room** option is enabled, anyone who joins the meeting 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.

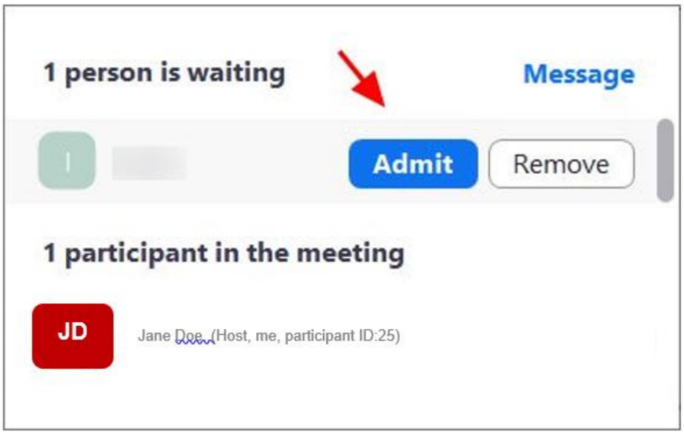

1 person is waiting
Message
I
Admit
Remove
1 participant in the meeting
JD
Jane Doe (Host, me, participant ID:25)

Figure 4: Admit Person into Meeting

4. Keep Zoom Client Updated

Make use of an updated Zoom application. 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.

With the increasing popularity of Zoom, cybercriminals will exploit its vulnerabilities. By installing the latest updates, your application will be protected.

5. Do not Share your Meeting ID

Each Zoom user is given a permanent **Personal Meeting ID** (PMI) which is associated with their account. If the PMI is shared with someone else, he/she will be able to check if there is a meeting in progress and potentially join it if a password is not set. Instead of sharing your PMI, new meetings can be created each time and shared with participants accordingly.

6. Disable Participant Screen Sharing

To prevent your meeting from being hijacked by others, participants (other than the Host) should be prevented from sharing their screens. As a host, this can be done in a meeting by clicking on the up arrow next to **Share Screen** in the Zoom toolbar and then clicking on **Advanced Sharing Options** as shown below.

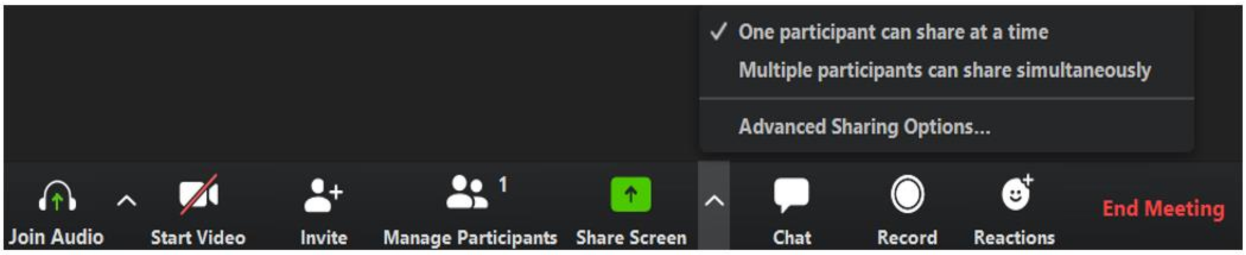
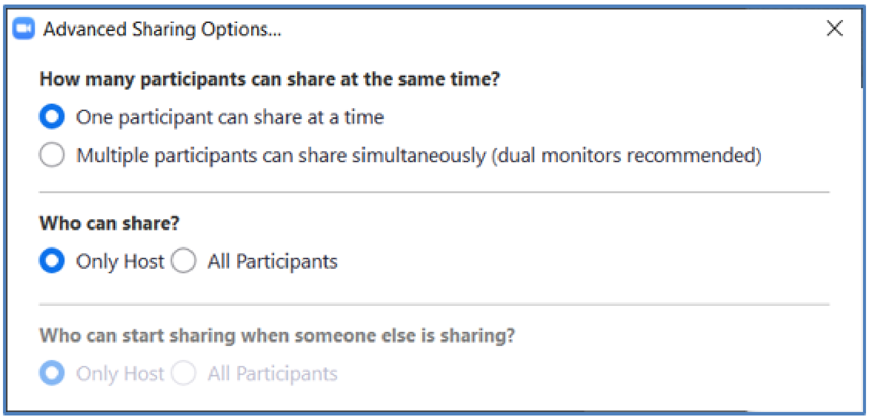

✓ One participant can share at a time
Multiple participants can share simultaneously
Advanced Sharing Options...
Join Audio
Start Video
Invite
Manage Participants 1
Share Screen
Chat
Record
Reactions
End Meeting

Figure 5: Advanced Sharing

When the Advanced Sharing Options screen opens, change the **Who Can Share?** setting to **Only Host**. This is shown below:



Advanced Sharing Options...

How many participants can share at the same time?

● One participant can share at a time
○ Multiple participants can share simultaneously (dual monitors recommended)

Who can share?

● Only Host ○ All Participants

Who can start sharing when someone else is sharing?

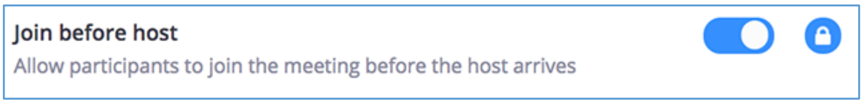
● Only Host ○ All Participants

Figure 6: Disable Participant Screen Sharing

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

7. Disable Join Before Host Feature

The **Join Before Host** option allows others to continue a meeting in the absence of an actual host. With this option enabled, the first person who joins the meeting will automatically be made the host and will have full control over the meeting.

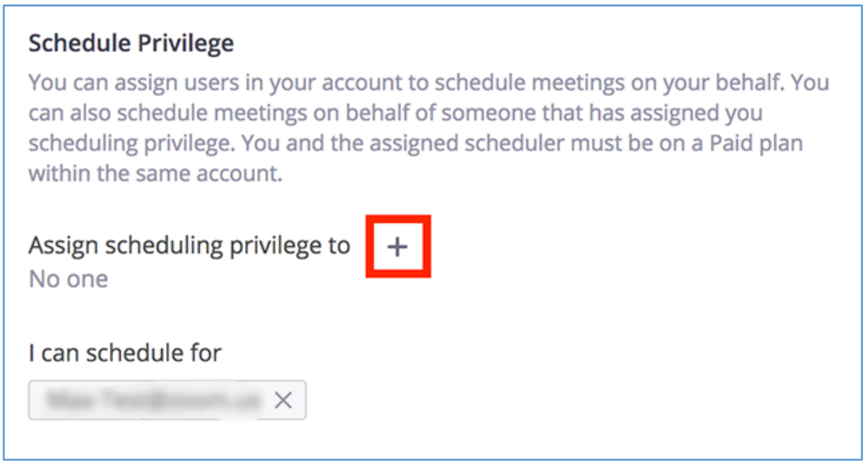


Join before host

Allow participants to join the meeting before the host arrives

Figure 7: Join before Host Toggle Locked

Alternatively, **Scheduling Privilege** may be given to a trusted participant to host the meeting in the absence of an actual host. This is shown below:



Schedule Privilege

You can assign users in your account to schedule meetings on your behalf. You can also schedule meetings on behalf of someone that has assigned you scheduling privilege. You and the assigned scheduler must be on a Paid plan within the same account.

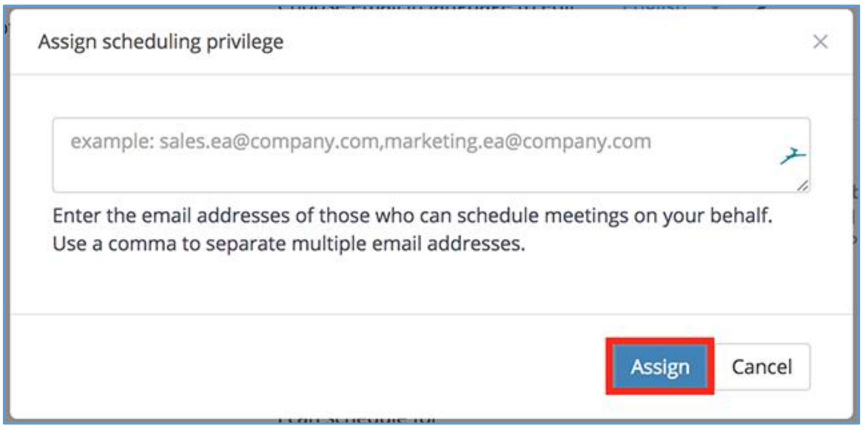
Assign scheduling privilege to +

No one

I can schedule for

[redacted] ×

Figure 8: Scheduling Privilege



Assign scheduling privilege ×

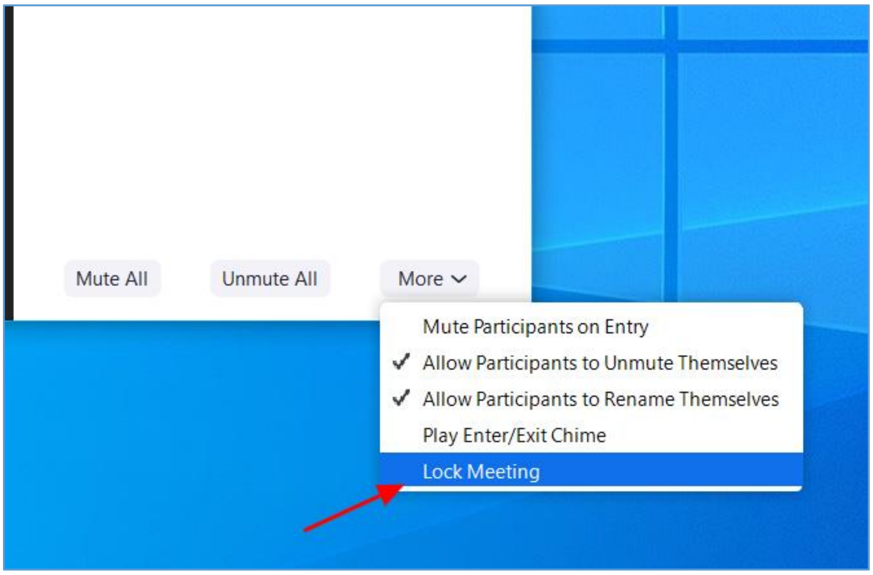
example: sales.ea@company.com,marketing.ea@company.com

Enter the email addresses of those who can schedule meetings on your behalf. Use a comma to separate multiple email addresses.

Figure 9: Assign Scheduling Privilege

8. Lock Meetings After Everyone has Joined

Once every participant has joined the meeting, you should lock the meeting to prevent unauthorized access. 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:

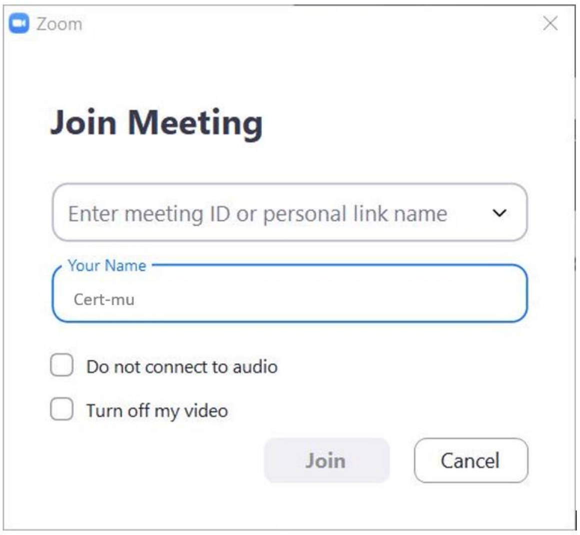


Mute Participants on Entry
✓ Allow Participants to Unmute Themselves
✓ Allow Participants to Rename Themselves
Play Enter/Exit Chime
Lock Meeting

Figure 10: Lock Meeting

9. Do not post pictures of your Zoom meetings

If a picture of your Zoom meeting is taken and posted online, the associated meeting ID will be displayed. The meeting ID can be used to gain unauthorized access to the meeting by manually joining the displayed ID. It is therefore advised not to post pictures of meetings using Zoom.



Enter meeting ID or personal link name

Your Name: Cert-mu

□ Do not connect to audio
□ Turn off my video

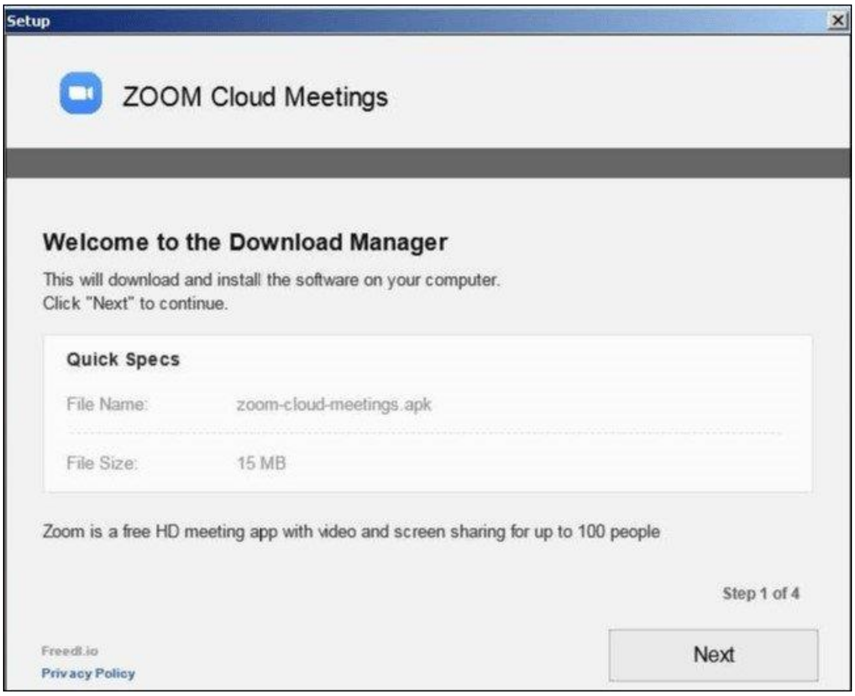
Figure 11: Manually Joining Meeting by ID

10. Do not post Public Links to your Meetings

When creating Zoom meetings, it is advised not to publicly post a link to your meeting. If links are posted publicly, search engines such as Google will be able 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, if a person has your Zoom link they can Zoom-bomb your meeting.

11. Watch out for Zoom-themed malware

With the Coronavirus outbreak, illicit cyber activities such as malware, phishing scams and other attacks related to the pandemic are on the rise. This also include malware and adware installers being created that pretend to be Zoom client installers. An example is shown below:



Setup

ZOOM Cloud Meetings

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

Step 1 of 4

Figure 12: Malicious Zoom Installer

References

- https://www.itu.int
- https://www.unicef.org
- https://www.bbc.com
- https://ciso.economictimes.indiatimes.com
- https://www.weforum.org
- https://www.microsoft.com
- https://www.pcr-online.biz
- https://www.financialexpress.com
- https://www.indiatoday.in