Protect you Zoom meetings and class sessions (avoid Zoombombing)

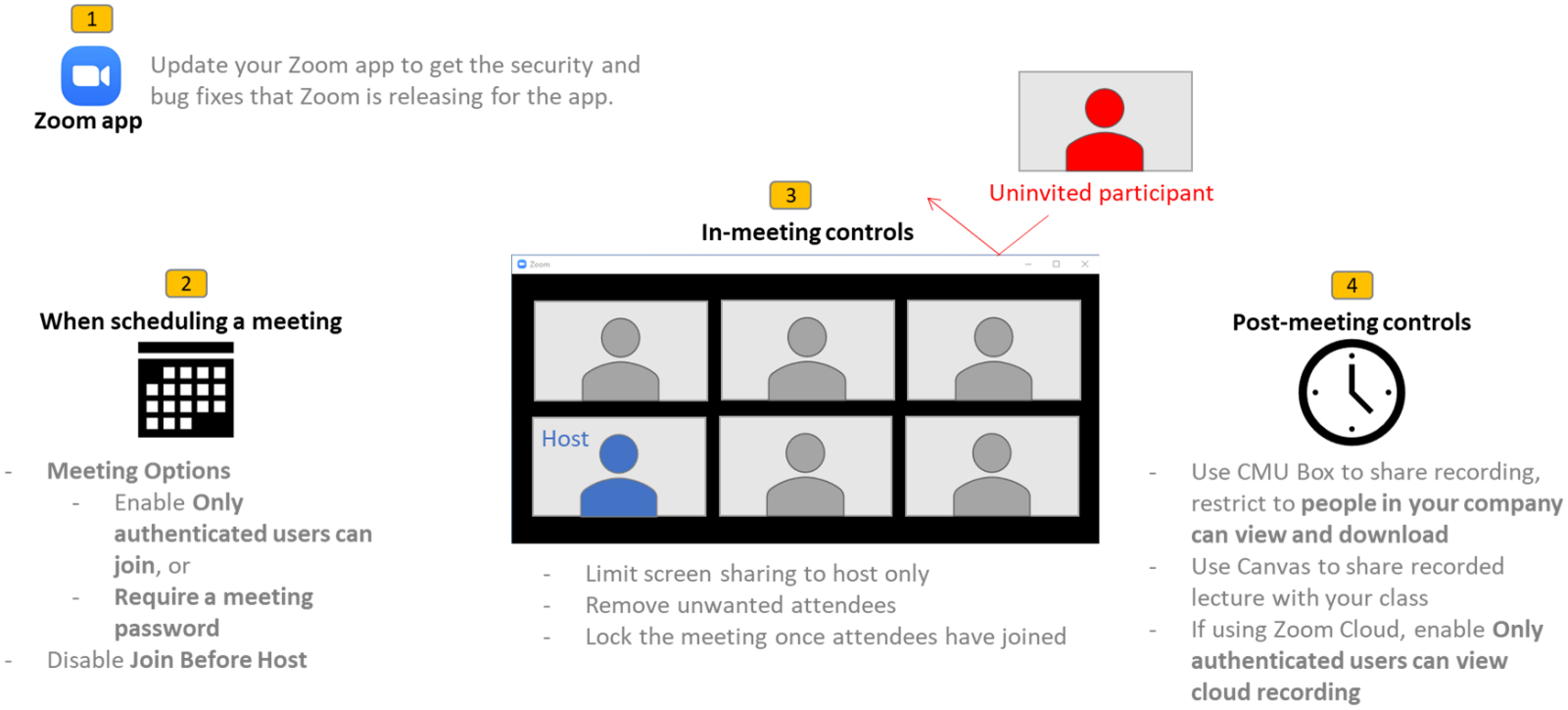
Recent media reports have highlighted privacy and security concerns about Zoom. This email provides you actionable advice on securing your Zoom meetings.

Zoom's default meeting settings allow anyone with the link or meeting ID to join that Zoom meeting. It is possible for an uninvited person to join a Zoom meeting and disrupt your class sessions, including the sharing of inappropriate images via screen sharing.

Zoom security options

Zoom offers a number of security options to prevent uninvited people from joining your meetings. You can apply these security options to previously scheduled meetings or when scheduling a new meeting. Some security options are available only through the Zoom web portal at https://cmu.zoom.us.

The following diagram shows you four steps to secure your Zoom call.



Update your Zoom app

Zoom is rapidly addressing security issues therefore it is necessary to keep your Zoom app updated to the latest version. To update your Zoom app:

1. Login to your Zoom desktop app using SSO (enter cmu.zoom.us at start)
2. Click on your name's initials in the top left of the **Home** screen
3. Select **Check for Updates**
4. Zoom will then check for available updates and download the latest version, if one is available
5. Once the download is complete, click **Update Now**

Schedule Meeting Settings

Enable security options when you schedule a new meeting or edit the security settings for previously scheduled meeting via CMU Zoom Web portal. These settings will ensure unauthenticated or uninvited people cannot join.

1. Browse to https://cmu.zoom.us
2. **Sign in** using your Andrew ID
3. Click **Meetings** (left menu) and then you can either schedule a new meeting or edit a previously scheduled meeting
4. On the **Schedule Meetings** page/screen enable *one* of the following (Recommended):
    - In the **Meeting Options** section, enable **Only authenticated users can join** option to limit access to individuals with **CMU Authenticated Zoom Accounts**. If non-CMU participants are invited to the meeting, select **Any Authenticated Zoom Account** option which will restrict participants to those with Zoom accounts (i.e., no anonymous participation).
    - Or, in the **Meeting Password** section, enable **Require meeting password** to assigns a strong password to your meetings and includes the details in the Zoom invite. This is the preferred method for meetings with non-CMU participants.
5. In **Meeting Options**, disable **Join Before Host**. If this option is not select then the participants can have the meeting without the host. You can make this the permanent default option by going to **Settings** in the left panel and disable **Join before host**.

In-meeting Controls

If you schedule the meeting with above recommended settings, you should not have any uninvited participants. Here we present further controls to deal with attendees who misbehave.

1. Start your meeting with the option to limit sharing to the host, and provide participants with sharing capability when necessary during the meeting. The steps are: next to **Share Screen**, click the up-arrow, select **Advanced Sharing Options**, under **Who can share**, click **Only Host**.

2. Remove an unwanted attendee from a Zoom Meeting: click **Manage Participants** from the meeting controls, the Participants panel will be visible, move your mouse over the unwanted participant name, click **More** button, select **Remove**.

3. Lock your meeting once all attendees join. No one can join a locked meeting, and the host will NOT be alerted if anyone tries to join. This option is recommended for discussing sensitive information with limited number of people. To lock a meeting, click **Manage Participants** from the meeting controls, the Participants panel will be visible, at the bottom right click **More**, select **Lock Meeting**.

Post-meeting Controls

If you recorded the Zoom meeting, you can share the recording in three places. Each must be secured properly.

1. CMU Box is recommended to share recorded meetings and lectures. When sharing please set the permissions of the Box link for the folder with the recording to **people in your company can view and download**.
2. Canvas is recommended to share recorded lectures. Just upload and make it visible to your students. Canvas' default controls already limit to your class.
3. Zoom Cloud can also be used to share recorded meetings and lectures. You must restrict access to the recording by signing in to https://cmu.zoom.us, click **Settings** in the left panel, click **Recordings**, and enable **Only authenticated users can view cloud recordings** (it is disabled by default).

Recent Zoom privacy and security concerns

April 6, 2020

There are several media reports raising privacy and security concerns about Zoom. This section presents Carnegie Mellon University Qatar (CMU-Q) Information Technology department's assessment of these concerns for our faculty, students and staff. We arrived at our assessment after an in-depth review of original stories, analyzing their substantial claims, weighing the potential impact on our campus, reviewing mitigation steps taken by or promised by Zoom to finally arrive at a short mitigation and clarification below. If you are interested in learning the details of any of this, please contact us at helpcenter@qatar.cmu.edu and we'll be happy to discuss with you further.

CMU-Q's Zoom service is under the main campus contract which has clauses for FERPA compliance that Zoom has agreed to adhere to. This commit Zoom to ensuring the confidentiality and security of data related to our use of Zoom at a level compliant with the FERPA law. So mere exposure of information to Zoom is not itself a concern in our context.

In the table below, we present name each risk in simple and brief language. The priority reflects the potential seriousness and impact of the risk. Priority should not be confused with the likelihood of the risk coming true. Status indicates where the risk stands. You will note that the statuses of these items are nearly all resolved, mitigated, not relevant, or not issues for our use case. Mitigations and clarification column contain a brief note with details.

No	Risk	Priority	Status	Mitigation and clarification
1	Zoombombing	1	Mitigations available	Mitigations are through various meeting schedule time and call time settings. These mitigations have been covered earlier in this document.
2	Calls are not end-to-end encrypted (Zoom can access unencrypted video). Chat is end-to-end encrypted	1	Confidentiality assured by Zoom FERPA compliance	Does not affect teaching and meeting use since the CMU agreement with Zoom binds them to ensure privacy compliant with FERPA requirements.
3	Video encryption is used in a mode (ECB) that may leak data	1	Encryption is sufficiently strong	While encryption scheme used by Zoom is not optimal, but it is still strong encryption. We deem it sufficiently strong for CMU-Q needs.
4	Windows UNC (universal naming convention) paths in chat are turned into clickable Windows actions. A participant click may result in inadvertent sharing of user's encrypted hashed credentials	1	Resolved	Resolved by a Zoom patch.
5	Encryption keys may be stored on a server in China	1	Resolved	This was a misconfiguration and has been rectified by Zoom.
6	Attention tracking lets a host know if Zoom is not the foreground application during screen sharing by showing indicators in participant panel.	2	Resolved	This option has been removed.
7	Data sharing (unauthorized) with LinkedIn Sales Navigator	2	Resolved	Zoom and LinkedIn have stopped the data sharing.
8	Private chats between two participants may be downloadable by the host.	2	Resolved	Does not seem possible. We tested and only saw the public messages and the host's own private messages were downloaded.
9	Privacy practice that seems to give the company permission to mine messages and files shared during meetings for ad targeting.	3	Resolved	Zoom states: we have never sold user data in the past, and have no intention of selling users' data going forward. Also, CMU-Q agreement binds Zoom to FERPA compliance.
10	Zoom does not publish a transparency report so governments' asking Zoom for data will be difficult to know and determine.	3	Very low priority concern for us	Zoom has pledged to publish a transparency report.
11	Zoom publishing email address and photo used by a user to anyone with same domain (e.g., abc@protonmail.com, 123@protonmail.com) and permits direct video calls.	3	Not relevant	We all use @andrew.cmu.edu version of our email address and calling within the CMU community is OK and desirable.

12	iOS app was sending analytics data to Facebook. Data includes time app was opened, user's time zone, city and device details.	3	Resolved	Resolved by Zoom removing the use of Facebook SDK (for the login with Facebook feature). SDK was sending device demographics data to Facebook.
13	Zoom was installing a web server on Macs to ease launch of Zoom from a web link	3	Resolved	Resolved in July 2019
14	Zoom installs on Mac without user clicking install	3	Resolved	Not an issue for us since we prefer the Mac Zoom app to be used instead of the browser.