**Best Practices for Zoom Conferencing:**

1. **Use a Random Meeting ID in Zoom** – learn more [here](https://support.zoom.us/hc/en-us/articles/201362413-Scheduling-meetings?zcid=1231)
	* It's best practice to generate a random meeting ID, so it can't be shared multiple times. This is the better alternative to using your [Personal Meeting ID](https://support.zoom.us/hc/en-us/articles/201362843?zcid=1231), which is not advised because it's basically an ongoing meeting that's always running.
2. **Use passwords to protect your meeting – and never share your meeting ID**
	* Do not share meeting ID and passwords, or pictures of your Zoom meetings, on any social media or public platform.
	* Ensure that the meeting ID and password are sent directly to intended attendees.
3. **Control Screen Sharing in Zoom** – learn how [here](https://support.zoom.us/hc/en-us/articles/360041591671?zcid=1231&_ga=2.241134720.2080525989.1585628198-352930134.1584722207)
	* Prevent participants from screen-sharing during a call using the host controls at the bottom. Allow sharing on a case-by-case basis. Use this option if you want to control the content shared during the meeting.
4. **Remove Unknown Participants in Zoom** – learn how [here](https://support.zoom.us/hc/en-us/articles/115005759423-Managing-participants-in-a-meeting?zcid=1231&_ga=2.2436403.2080525989.1585628198-352930134.1584722207)

By default, if you remove participants or panelists from the webinar, they won't be able to rejoin using the same email address.

* If the Participants panel is not visible, click Manage Participants at the bottom of the Zoom window.
* Next to the person you want to remove, click More.
* From the list that appears, click Remove.
1. **Lock Your Meeting in Zoom** – learn how [here](https://support.zoom.us/hc/en-us/articles/201362603-What-Are-the-Host-Controls-)

The [Zoom Host Controls](https://support.zoom.us/hc/en-us/articles/201362603-What-Are-the-Host-Controls-) allow the host or co-host to lock the meeting. Once all your attendees have joined,

* If the **Participants** panel is not visible, click **Manage Participants** at the bottom of the **Zoom** window.
* At the bottom of the **Participants** panel, click **More**.
* From the list that appears, click **Lock Meeting**.

Unlock the meeting following these same steps.

When a meeting is locked, no one can join, and you (the host or co-host) will NOT be alerted if anyone tries to join, so don't lock the meeting until everyone has joined.

1. **Keep the Zoom App on Your Devices Updated**

Similar to any other application, it is important to keep the app up to date to protect it from the latest vulnerabilities. **If you having trouble updating via the methods below, you can always download the latest version of zoom** [**here**](https://support.zoom.us/hc/en-us/articles/201362233-Where-Do-I-Download-The-Latest-Version-).

*Windows and MacOS Instructions*:

The latest version update information of Zoom for Windows can be found [here](https://support.zoom.us/hc/en-us/articles/115002847143-New-Updates-for-Zoom-Rooms-for-PC) / MacOS can be found [here](https://support.zoom.us/hc/en-us/articles/201361963-New-Updates-for-macOS).

* Open the Zoom app
* Click your user icon on the top right
* Click Check for Updates
* You will be prompted to update if out of date

*iOS Instructions*:

This will only apply if automatic updates are not enabled. The latest version update information of Zoom for IOS can be found [here](https://support.zoom.us/hc/en-us/articles/201361943-New-Updates-for-iOS).

* Open the App Store
* Search for Zoom
* If an update exists, Open will be replaced with Update. Click Update

*Android Instructions*:

* Open the Zoom app
* Click Settings
* Click About
* Click Version
* You will be prompted to update if out of date

**Actions by Zoom and TTUHSC to further secure Zoom conferencing**:

Zoom recently [updated the company's privacy policy](https://blog.zoom.us/wordpress/2020/03/29/zoom-privacy-policy/) to be more transparent about the data that it does collect. Furthermore, Zoom has offered clarification on [how encryption works within the platform](https://blog.zoom.us/wordpress/2020/04/01/facts-around-zoom-encryption-for-meetings-webinars/), acknowledging that it had at times implied that data was encrypted end-to-end.

1. **The addressable space for meetings insufficient (9 to 11 digit number), ‘war dialing’ or guessing the meeting ID through sequential iteration is possible.**
	1. *Action by Zoom* – None
	2. *Action by TTUHSC* - Ensure every meeting is password protected
2. **Zoom sending information to Facebook within Zoom app for IOS.**
	1. *Action by Zoom* – Removed Facebook software development kit from iOS app
	2. *Action by TTUHSC* – Ensure latest version of Zoom installed
3. **Zoom privacy policy too broad (allowed gathering of video sessions, contents of whiteboards, uploaded documents, instant messages, chat sessions, names of the individuals on the call, and contents of Zoom cloud storage)**
	1. *Action by Zoom* – No longer collects data
	2. *Action by TTUHSC* – None required
4. **Zoom marketed as End to End (E2E) encryption. Reports show use of simpler TLS security from endpoint to Zoom servers, decrypt – re-encrypt, then TLS back to the other endpoints.**
	1. *Action by Zoom* – Immediate statement, “Currently, it is not possible to enable E2E encryption for Zoom video meetings,” as well as, “When we use the phrase ‘End to End’ in our other literature, it is in reference to the connection being encrypted from Zoom end point to Zoom end point.”  However, on 1 April 2020, Chief Product Officer Oded Gal explained that Zoom operates something closer to the first kind of E2E system (centralized company management of keys) than the second (endpoint-only possession of keys). Zoom apparently *does provide end-to-end encryption between participants using Zoom native and Web apps*. The data passes across Zoom’s servers without decryption and re-encryption. However, in order to connect sessions to other kinds of services, Zoom operates “connectors” that will decrypt data in certain circumstances (phone connection, polycon, cloud recording).
	2. *Action by TTUHSC* – Password all events, enable waiting room, and password all phone connections.
5. **On 30 March 2020, it was identified that two “zero-day” bugs could expose Zoom’s Mac users to exploits. However, these exploits can’t be invoked remotely unless a malicious party could embed the exploit in software, they convince someone to download and install, such as a Trojan horse or malware disguised as something useful.**
	1. *Action by Zoom*: On 1 April 2020, Zoom updated its OSX app
	2. *Action by TTUHSC*: Ensure Zoom application is patched to the latest version

As always, we all need to remain extra vigilant during this time of unprecedented disruption in our professional and private lives. Please take precautions, keep calm, and Zoom safely.

<https://blog.zoom.us/wordpress/2020/03/20/keep-uninvited-guests-out-of-your-zoom-event/>