



Keeping Zoom Secure at Extension

Not all Zoom Accounts are the Same

Extension's use of Zoom is different than what the general public is using. Our Zoom accounts are bound together under a Zoom for Education enterprise account. This allows us to enforce certain security features and settings as well as provide us with reporting tools and a level of support that most personal Zoom accounts do not have access to. These settings cannot be overridden by the user, and include the following:

- Waiting Room enabled by Default
- Passwords required for meetings
- Join Before Host disabled
- Participant Screen sharing disabled at meeting start (can be changed by Host)
- Meeting chats cannot be saved
- File Transfer via chat disabled
- Cloud based meeting recording disabled - Hosts can record their meetings, but the recording is saved locally, not via Zoom's cloud storage

These best practices hold true not just for Zoom, but for any current videoconferencing platform. Providing a secure environment for both our staff and participants is critical, especially during our efforts around the pandemic.

Zoom's Data Encryption Model

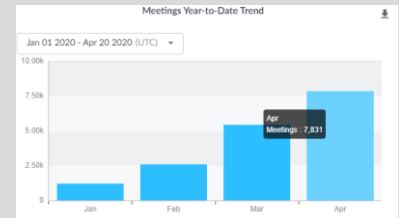
In early April 2020, Zoom was the topic of world-wide attention around issues related to data encryption and the location of their data centers. Zoom acknowledged people's concerns around data encryption methods and began making changes to address them immediately. Zoom has provided an in depth overview of their current encryption practices both on their website and in a detailed white paper:

<https://zoom.us/docs/doc/Zoom%20Encryption%20Whitepaper.pdf>

Extension's use of Zoom is for public outreach and programming efforts. Our internal training efforts reinforce this as our primary use for Zoom. We do not suggest the use of Zoom for any data which would meet data classification standards as restricted or sensitive data.

More than just Meetings

Extension has used Zoom to reach audiences around the state. We've leveraged our expertise to assist with training Election Poll workers, as well as provided Zoom based Board of Review training. We have utilized Zoom to move conferences to an online format, and we have enabled content experts to work with 4-H groups via a combination of Zoom and Livestreaming.



Zoom Use at Extension

We have adopted Zoom as our primary platform for collaboration and remote learning. As we've shifted our programming efforts to support our remote learners, our use of Zoom has grown considerably month to month, with our April numbers being on track for over 10,000 meetings.

Training is required

Extension staff are required to attend a Zoom training session prior to being given access to a licensed Zoom account. These trainings include best practices on both security and effective use of Zoom as a video conferencing platform and are integral for ensuring that our participants can have a secure and safe Zoom experience. Over 700 have registered for training since March.

Zoom Data Center Settings

In order to protect the integrity of any data transmitted over Zoom, at this time Extension is limiting our meetings and webinars to local, United States based data center regions. This is a setting which cannot be changed by our end users and is locked for all user accounts.

Select data center regions for meetings/webinars hosted by your account



Include all data center regions to provide the best experience for participants joining from all regions. Opting out of data center regions may limit CRC, Dial-in, Call Me, and Invite by Phone options for participants joining from those regions.

- | | |
|--|---|
| <input type="checkbox"/> Europe | <input type="checkbox"/> Hong Kong |
| <input type="checkbox"/> Australia | <input type="checkbox"/> India |
| <input type="checkbox"/> Latin America | <input type="checkbox"/> Japan |
| <input type="checkbox"/> China | <input checked="" type="checkbox"/> United States |
| <input type="checkbox"/> Canada | |

ZoomBombing – Video Conference Gate Crashing

Any time an online video conference system is used in a public facing environment, there is a risk of 'gate crashing' or 'ZoomBombing' by uninvited guests.

- Zoom identified the potential for this during the Summer of 2019 and took steps to address this by defaulting to requiring passwords for new meetings. <https://support.zoom.us/hc/en-us/articles/360033331271-Account-Setting-Update-Password-Default-for-Meeting-and-Webinar>
- Zoom Meeting IDs have been updated from 9 to 11-digit numbers as well in order to make it more difficult people to randomly join Zoom meetings.
- Our enforced account settings coupled with best practices shared during our trainings help to protect our staff and participants from ZoomBombing.

CDNs and Zoom

Within our administration tools, we have control over the use of Content Delivery Networks as well as whether China based CDNs are used. At this time, we are using the default, which is Amazon's CloudFront system.

Join via Browser

Zoom allows you to participate via browser. If you have to download Zoom, only do so via the official <https://zoom.us> website.

Meeting Registration

Extension has updated our training website to include information specific to running secure Zoom Meetings. We discourage users from sharing links to meetings via Social Media, and instead ask that they use a registration system

To learn more visit:

<https://fyi.extension.wisc.edu/edtech/zoom-training-information/>

For more information

Please visit <https://zoom.us/security> for additional insight on how Zoom is addressing security concerns.

If you have questions specific to the importance of Zoom within Extension currently, please reach out to Extension Technology Services directly.

Tony Roman
Educational Technology Support
Zoom Administrator
tony.roman@wisc.edu

Greg Johll
Educational Technology Support
Director
greg.johll@wisc.edu