IMPROVING ZOOM SECURITY
ZOOMBOMBING

Zoom at Texas A&M University offers several features and options that can help you maintain the security of your Zoom meeting. Use the following tips to help prevent Zoombombing, where uninvited users enter your Zoom meeting and use the screen share feature to display inappropriate content.

9 TIPS FOR PREVENTING ZOOM BOMING

1. UPDATE YOUR ZOOM CLIENT

Zoom regularly releases new versions of its desktop client and mobile app to fix bugs and improve security. These client updates are not always automatic. Make sure you keep your Zoom up to date, as this is one of the best ways to avoid Zoom Bombing.

To check if you need to update your Zoom client:

- Sign in to your Zoom desktop client.
- Click your profile picture and then click “Check for updates.”
- If there is a newer version, Zoom will download and install the newest version.

2. DO NOT PUBLICLY SHARE MEETING LINKS

This might seem like common sense, but only share meeting links with the people meant to be in the meeting. Don’t share them on public social media platforms like Facebook or Twitter.

3. DISABLE ‘JOIN BEFORE HOST’ FEATURE

The participants could be having a party without you there to monitor. If you disable Join before Host, the participants will see a pop-up box that says “The meeting is waiting for the host to join.” If you are the host, there is a login button to login and start the meeting as the host.

4. REQUIRE PARTICIPANT AUTHENTICATION

Zoom’s authentication feature allows the host to restrict participants who are able to join a meeting to only those logged into Zoom. If a participant isn’t signed in using their TAMU email address, they won’t be able to get in.

5. MUTE PARTICIPANTS UPON ENTRY

Barking dogs and other distractions can take over your meeting unintentionally. Consider disallowing participants to unmute themselves. With this feature enabled, participants can use the Raise Hand or Chat feature to indicate if they have questions. The host can then manually unmute individuals wishing to speak.

6. USE THE IN-MEETING SECURITY TAB

The Security icon in the meeting controls allows the host or co-host of a meeting to enable or disable options during a meeting to secure the meeting and minimize disruption during the meeting. Under the in-meeting security tab:

- Disable Waiting Room
- Disable Share Screen
- Disable Unmute Themselves
- Disable Annotate During Screen Share

7. FILE TRANSFER

The ability to send files to your participants during a meeting can be helpful. This feature can turn problematic if a participant sends unintentionally or inappropriate files/gifs/images to other meeting participants. To prevent this, disable file transfer for participants, upload files that you want to share on Google Drive or Office 365, and provide participants links to these files.

8. PRIVATE CHAT

The Chat feature is a great way to facilitate in-meeting participant engagement. Disabling private chat will eliminate a back channel where possible bullying or harassment during your meeting may occur.

9. WHEN IN DOUBT, KICK THEM OUT!

If a disruptive participant manages to get into your meeting, you have the ability to remove them. To do so, click the Participants tab, then mouse over the disruptive participant's name and select Remove. Once removed, the participant will not be able to rejoin.

ADDITIONAL ZOOM RESOURCES

- Update to the Latest Version of Zoom
- In-meeting Security Options
- Sending a file in a Meeting
- Managing Participants in a Meeting

For further assistance, please contact the Office for Academic Innovation Service Desk.