Securing Zoom Meetings

There has been a lot of news attention regarding Zoom being insecure and meetings being invaded by “Zoombombers.” Like any tool built to provide collaboration capabilities to groups of people, there is some risk in using Zoom. However, organizers of Zoom meetings can *significantly* decrease the chance that their meetings are compromised by setting them up using the guidelines below. Additional information, including how to configure meeting passwords, can be found on Zoom's Meeting and Webinar Passwords page.

ITS **strongly** recommends the following meeting settings to avoid malicious activity during your meetings:

- Automatically Generate a Meeting ID
- Require Meeting Password
- Enable the Waiting Room Feature
- Disable “Join Before Host”
- Limit Screen Sharing to Host
- Remove Participants from Meetings
- Lock the Meeting
- Record Meeting Automatically
- Other Considerations
- Getting Help

Consider Where Applicable

These guidelines may not be practical for all meetings. Organizers should consider the intent of the meeting, what features are needed for it to productive, and the sensitivity of the content of the meeting when configuring options for a meeting to balance risk with productivity.

Automatically Generate a Meeting ID

Your Personal Meeting ID (PMI) may accidentally be made public. Therefore, when configuring the meeting ID, select “Generate Automatically.” This ensures that a unique meeting ID is used for every meeting.

Require Meeting Password

Under “meeting options” select “Require meeting password,” then choose a password of at least 8 characters and a mix of upper case, lower case, numbers, and symbols. Participants will need to provide this before joining the meeting.

This password will be placed in the invite email by default. Organizers of highly sensitive meetings should consider removing this password from the invite before sending it out and distributing the password via a text message or telephone call.

Enable the Waiting Room Feature

Turning on the waiting room feature allows the meeting organizer to admit people as they arrive. This will significantly reduce the chance that unwanted attendees will be able to join the meeting.

Disable “Join Before Host”

Although this option is convenient if the organizer of the meeting is late to the meeting, when this is enabled, the first person to join the meeting is made host and has total control over the meeting.

Limit Screen Sharing to Host

By default, only the host is permitted the ability to share a screen. This helps prevent bad actors from sharing screens with inappropriate content. During the meeting, the host may grant permission to additional users if need be. When practical, this setting should be left as default, but some meetings may require numerous attendees to share their screen in which case organizers may consider de-selecting it.

Remove Participants from Meetings

If an unwanted attendee has joined a meeting, the meeting host may remove that user through the Manage Participants panel.

Lock the Meeting

Hosts and cohosts may choose to lock a meeting once all expected attendees have joined. This prevents unwanted attendees from attempting to enter and disrupt the meeting.

Record Meeting Automatically

This feature is turned off by default. If organizers turn this feature on, they will have the option to select “locally” or “in the cloud” to save their meetings. If a meeting contains any sensitive information, and until Zoom security is better understood, organizers should select “locally” instead of “in the cloud” and then share the recording through a University managed system such as shared drives or One Drive.

Other Considerations

- Keep in mind that Zoom meetings are as secure as the email that is used to send the invite. Organizers of highly sensitive meetings may wish to verify (by voice or video) that attendees are who they expect them to be.
- Even if you, as the organizer, are not recording the meeting, attendees may have software on their systems that allow recordings of their screen or videos. You may want to clarify at the meetings beginning that no recordings are permitted.

Getting Help

For support on the information above, contact the ITS Help Desk by calling at 315.443.2677 or by emailing help@syr.edu.

Top