Best Practices for Zoom Privacy and Security

The University of Dayton IT team has configured Zoom's privacy and security settings to reduce the possibility of unknown or unwelcome guests joining a meeting or webinar.

The measures explained in this document will increase the security of your Zoom sessions and reduce the chance of unwanted attendees. ***We recommend using as many of these options as you reasonably can without impacting your meeting operations.*** If you are discussing any sensitive or confidential information in your meetings, these measures become more important.

Remove a Participant from a Zoom Meeting or Webinar

If you have already begun a session and find an unwanted attendee has joined:

1. If the Participants panel is not visible, click **Manage Participants** at the bottom of the Zoom window.
2. Next to the person you want to remove, click **More**.
3. From the list that appears, click **Remove**.

Enable the Waiting Room Feature

The Waiting Room feature allows the host to control when each participant joins the meeting. As the meeting host, you can admit attendees one by one, or hold all attendees in the virtual waiting room and admit them all at once. This requires more work by the host, but only allows participants to join if you specifically admit them.

Disable Join Before Host

If you are scheduling a meeting where sensitive information will be discussed, it's best to leave **Enable join before host** (found when scheduling a meeting) turned off. Visit Zoom's Join Before Host help page for more information.

The **Join Before Host** option can be convenient for allowing others to continue with a meeting if you are not available to start it, but with this option enabled, the first person who joins the meeting will automatically be made the host and will have full control over the meeting.

Another option is to assign an Alternative Host.

Limit Sharing to the Host

While in your meeting,

1. Click the up-arrow next to Share Screen.
2. Select Advanced Sharing Options.
3. Under Who can share, click Only Host.

This won't be appropriate when multiple participants will need to share and collaborate, but setting this restriction will prevent unwanted guests from interrupting the meeting by initiating intrusive sharing.

Meeting Passwords

For maximum security, it is recommended that you set a strong password for all meetings and webinars.

When scheduling a meeting, select **Require meeting password**, then specify a strong password (make your password at least eight characters long and use at least three of the following types of characters: lowercase letters, uppercase letters, numbers, symbols). Participants will be asked for this password in order to join your meeting.

Needless-to-say, you want to communicate the password to your participants in a secure fashion.

Lock Your Session

The Zoom Host Controls allow the host or co-host to lock the meeting. Once all your attendees have joined,

1. If the **Participants** panel is not visible, click **Manage Participants** at the bottom of the **Zoom** window.
2. At the bottom of the **Participants** panel, click **More**.
3. 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. Participants that leave will also be unable to rejoin.

For additional assistance with Zoom, including best practices advice, please contact the University of Dayton IT Service Center at itservicecenter@udayton.edu or 937-229-3888.

For specifics use cases regarding learning and teaching, please contact the Office of eLearning at elearning@udayton.edu or 937-229-5039.

You may also refer to eLearning's Zoom documentation or Zoom's own help documentation.

University of Dayton