

Toolkit for Zoom Meetings

There is no one-size-fits-all instruction for every meeting. Each meeting must decide which security tools to use to balance safety in the meeting with welcoming the newcomer.

Security Tips

- **Assign** a [Zoom Host & Co-host](#), one to chair the meeting and one to manage muting, hand-raising, and handle meeting intrusions.
- **Disable** [Join Before Host](#) to keep users out before the host arrives.
- **Mute** upon entry and [Disable self-unmuting](#).
- **Restrict** [In-Meeting Chat](#) to Host Only only during the meeting. Many meetings open it up for fellowship after the meeting.

If a Troll disrupts your Meeting

- **Disable** [Screen Sharing](#) (or select “host only”) to prevent trolls from hijacking the screen
- **Disable** [Virtual Background](#) to prevent trolls from using offensive images as their background.
- **Remove** [Unwanted Participants](#) by clicking “Manage Participants,” scrolling over participant’s icon, click More>Remove.
- **Disable** [File Transfer](#) to prevent trolls from sending files to the whole group.

Best Practices

- **Use the Hand Raise** feature (in Participant mode) so the host is in control of who shares
- **Use** “Only Authenticated Users Can Join” which means participants sign up for a FREE Zoom account. It’s just more secure.
- **Lock the meeting** at a certain point to prevent anyone else from joining

Useful Links

Zoom has a great [Getting Started](#) page and a [Safety Blog](#).
Cornell University has an informative [Zoom Safety Page](#)
NPR segment with lots of up-to-date info about [Zoom security problems](#)

Tradition 12

“Anonymity is the spiritual foundation of all our traditions, ever reminding us to place principles above personalities.”

Zoom and other virtual platforms are designed for easy connection, not anonymity. Our community--individuals, groups, trusted servants--can take time to PAUSE

and to THINK when making decisions about how to connect in the virtual world.