Zoom: Security

Last Modified on 03/15/2024 3:50 pm EDT

As one of the most popular web-conferencing tools, Zoom has become a target for online attacks. In addition, Zoom, as an outside vendor, can choose to share user data with other companies. For these reasons, we recommend doing the following in order to use Zoom securely.

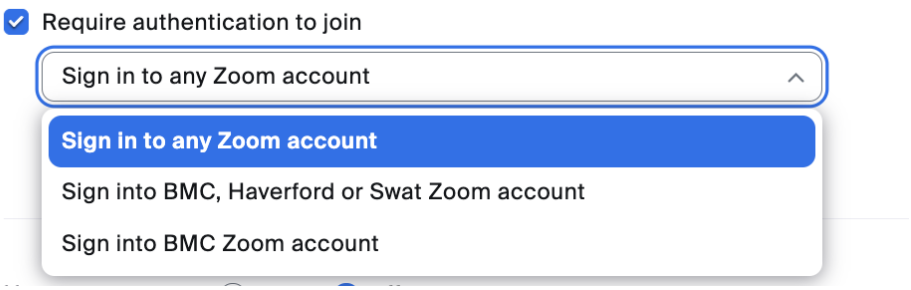
Prevent Zoom bombers

Zoom bombing occurs when an unwanted participant joins a meeting and disrupts it through inappropriate behavior such as yelling obscene language or sharing inappropriate materials. These attacks exploit Zoom's default meeting settings, rather than security gaps in the software itself.

Before a Meeting

Zoom has responded to the threat of Zoom bombing by making defaults for educational licenses such as Bryn Mawr's more restrictive. When scheduling a meeting, **please do not change the following default settings**. They are designed to keep Zoom bombers out of your meeting:

- **Randomly generated meeting ID**: When you create a new meeting, Zoom generates a random meeting ID number. Use this instead of your Personal Meeting ID, which remains the same from meeting to meeting and is therefore more vulnerable to being shared with unwanted guests.
- **A "waiting room" for all participants:** When the "waiting room" setting is enabled, hosts have to manually admit participants before they can join a meeting. By leaving this setting on, you can block anyone from joining a meeting who shouldn't be there.
- **Disabling of the "Allow participants to join anytime" setting:** This prevents anyone from joining the meeting before you start it.
- **Restrict attendance to people who have logged in with a Bryn Mawr or Tri-Co Zoom account:** Go to **Security > Require Authentication to Join** within your meeting settings to turn this feature on. Then, select **Sign into BMC Zoom account** or **Sign into BMC, Haverford or Swat Zoom account** from the drop-down menu.



Note: If you are unable to join a meeting where the host has required authentication with a BMC or Tri-Co account, make sure you are logging in with your college Zoom account instead of a personal one. Bryn Mawr students should read check if you are signed in with a BMC account for more information.

In addition, make sure to share your meeting link carefully once it's created. Anyone who has this link will be able to join the meeting, even if you've added a password to it. In fact, Zoom embeds the meeting password into the meeting link (look for "?pwd=" in the meeting URL if you don't believe us!).

If you need to advertise a Zoom meeting publicly (e.g., on a webpage), turn on**Require registration** and share the *registration link* instead. Participants will need to sign up with a working email address to receive the meeting link, which is usually enough to deter trolls. (See Zoom: Use registration to secure meetings for more information)

During a meeting

Once a meeting has started, hosts and co-hosts can also limit participant behavior during a meeting in ways that prevent Zoom bombing:

- Zoom has grouped many of the relevant permissions under **Security.** For convenience, click on this button and uncheck options under "Allow participants to." This will immediately disable them for everyone in the meeting. These options include the following:
  - Share Screen
  - Chat
  - Rename Themselves
  - Unmute Themselves
  - Start Video
  - Share Whiteboards
  - Share Notes
  - Start Recordings Local Files
  - Request Recording Permission
  - Set Meeting Timers
- To grant or remove permissions for individual participants, click **Participants > More.** This will open a menu where you can limit individual participant's permissions.
- Click **Screen Sharing**, to open the **Advanced Sharing Options** menu. From there, change **Who can share?** to "Host Only."

Remove disruptive users

Responsibly share Zoom recordings

Keep your Zoom app up-to-date

Third-party integrations and privacy concerns

Videos and further Reading on Zoom Security

- **Zoom:** Using host and co-host controls in a meeting

Questions?

If you have any additional questions or problems, don't hesitate to reach out to the **Help Desk**!

Phone: 610-526-7440 | Library and Help Desk hours
Email: help@brynmawr.edu | Service catalog
Location: Canaday Library 1st floor