Zoom: Security

Last Modified on 08/11/2022 9:43 am EDT

As the most popular web-conferencing solution on the market (some industry analyses estimate it has almost double the market share of competitors like Go To Meeting), Zoom has become a target for online trolling attacks. Zoom is also facing several investigations and lawsuits about the transparency and security of its practices for sharing data with third party applications like Facebook. This article discusses things you can do to use Zoom securely.

See also:

- Zoom's Security page provides information and updates about about what the company is doing to improve security.

Protection against Zoom-trolling/bombing

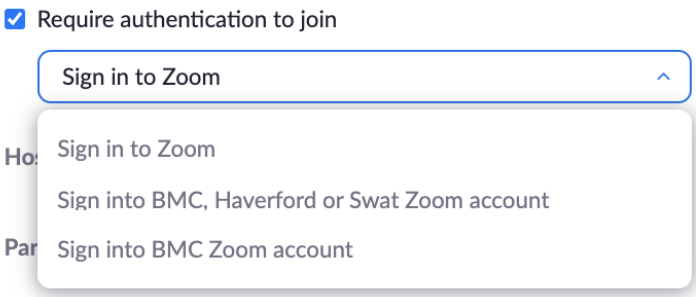
Trolling attacks have so far stemmed from exploitation of Zoom's default meeting settings, rather than security gaps in the software itself. Zoom has responded by making defaults for educational licenses such as Bryn Mawr's more restrictive.

Keep trolls out

Hosts can take these steps to *make it harder for trolls to find/enter meetings.*

- Use a randomly generated meeting ID (default for scheduled and instant meetings) rather than your Personal Meeting ID. Personal Meeting IDs remain the same from meeting to meeting and are therefore more vulnerable to exploitation.
- Keep the "waiting room" enabled for all participants. A host will have to manually admit participants before they can join the meeting and this gives you the most control over who gets in.
- Be careful about sharing Zoom meeting or webinar links and *don't post them publicly* (i.e., on a web page that anyone can access).
    - By default Zoom embeds the meeting password into the auto-generated meeting link (look for ?pwd= in the link). This enables participants to join by simply clicking the link, *but it means that anyone who has the link can join.*
    - If you need to advertise a Zoom meeting publicly (e.g., on a webpage) or very widely (e.g., to a very large mailing list), turn on **Require registration** for the meeting the 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)
- Leave the **Allow a removed participant to rejoin** *disabled* in your **In Meeting (Basic)** settings. If you ever need to *remove* a disruptive participant from a meeting, this will prevent them from rejoining. (Note: it does not impact people who voluntarily leave a meeting and then rejoin.)
- You can restrict attendance to people who have logged in with a Bryn Mawr (or Tri-Co) Zoom

account using the **Security > Require Authentication to Join** meeting setting.



- Note that if you enable this, legitimate BMC or Tri-co participants will be unable join if they try to do so while *logged into a personal Zoom account*; they will see an alert stating the meeting is for authorized users only.
- If you are unable to join a meeting and 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. In Bryn Mawr's case, you must use the **Login with SSO** option to sign in; if you log in any other way, you are using a personal account, even if it is attached to a brynmawr.edu email address. Check if you are signed in with a BMC account.

Limit what trolls can do: Before a meeting

Hosts can make it harder for trolls disrupt a meeting if they *do* get in by disabling features they don't need. If you are concerned about Zoom bombing, adjust your default **Meeting Settings** so that the meetings you host start with participants able to do fewer things. You can always enable features *during* a meeting if you find you need them.

To edit your default meeting settings:

1. Go to brynmawr-edu.zoom.us and **Log in with SSO**.
2. Click **Settings** in the left sidebar.
3. Click **In Meeting (Basic)** to jump down to that subset of settings.
4. **Disable** the following features by clicking the switches next to them until they are in the off/left position (font name="toggle-off") and gray. (Switches for enabled features are in the on/right position ([font name="toggle-on"]) and blue).
    - **Chat**
    - **File transfer**
    - **Annotation**
    - **Whiteboard**
    - **Allow removed participants to rejoin** (Note: this only affects participants whom a host or co-host removes. Participants who drop out due to tech issues or voluntarily leave will still be able to rejoin.)
    - **Allow participants to rename themselves**
5. Under **Screen Sharing**, change **Who can share?** to **Host Only**. As host you will still be able to permit participants to share their screens during the meeting, but the participants will not be able to initiate screen sharing themselves.

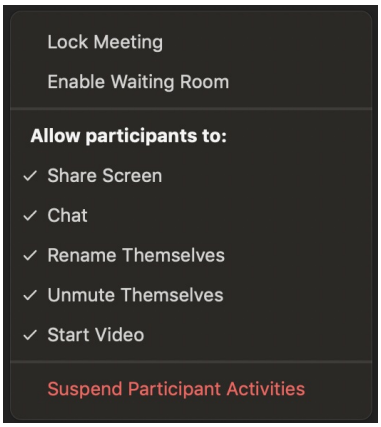
Note: Don't worry if you Modified/Reset text appears or disappears as you turn features on and off.

When you see this text, it means the settings you choose are different from those our Zoom admins have chosen for the College as a whole. Zoom admins are trying to balance security and collaboration needs of all users in all use cases — the settings we choose may not be ideal for everyone.

Limit what trolls can do: During a meeting

Hosts and co-hosts can also limit *participant behavior during a meeting.*

- Zoom has grouped many of the macro-level permissions under **Security**, for convenience click on this button and uncheck options under **Allow participants to** immediately disable them for everyone in the meeting, as shown below.



- To grant or remove permissions for individual participants, hover over their name in the **Participants** panel and click **More ...**

See also:

- Host and Co-Host Controls in a Meeting shows a video tour and details on everything you can do to manage participants.

Remove disruptive users

If you suspect you are being Zoom-bombed, the host or co-host should immediately

1. Click the **Security** button and then the red **Suspend Participant Activities** text to *immediately.*
   - Stop all participants from sharing video, audio, and screens.
   - Turn off the chat and annotation features.
   - Close breakout rooms.
   - Turn off all recordings.
2. Zoom will prompt you to report the disruptive participants, who will be removed from your meeting and will not be able to return (unless you've enabled **Allow removed participants to rejoin** for all meetings).

3. The meeting will resume, and you will be able to turn on the disabled features one-by-one as needed.

If you wish to exclude participants from a meeting without suspending it:

- Click **Manage Participants**, hover over their name, click **More** and choose **Remove** from the drop-down menu.
- Click **Lock Meeting** to prevent new participants from joining a meeting, even if they have the link and passcode.

Responsibly share Zoom recordings

In spring 2020 there were reports of Zoom meeting recordings showing up in online searches. These seem to have involved recordings that were posted to streaming services such as YouTube using filenames that searchers were able to guess.

If you need to create and share recordings of Zoom meetings, LITS recommends:

- Always inform meeting participants that you are recording and *how you intend share/publish the recording*.
- Share through Panopto, rather than Zoom Cloud. We have set up a connection between Zoom and Panopto, so that when you choose "record to Cloud" in Zoom the recording is automatically transferred to Panopto and only shared with meeting participants.
- No matter you store recordings*, always delete them once you no longer need them*. The longer a file remains on the Internet, the more opportunities there are for it to be hacked.

Keep your Zoom app up-to-date

Like most software publishers, Zoom provides regular software updates, which may include fixes for security issues.

- If you are prompted to install an update with you open or close the Zoom app, do it!
- In the desktop app (Mac or PC), you can click on your user icon and choose **Check for Updates** to manually check for and install updates.

Third-party integrations and privacy concerns

The College is being very careful and conservative about third-party integrations with our institutional Zoom license:

- We have disabled the options to log in with Google and Facebook.
- We will only enable integrations for platforms with which the college has a contractual relationship that included a review of data security and privacy policies, and then only if integration provides substantial functionality benefits.

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