-->

Zoom Security Guidelines

Last Modified on 10/23/2025 12:00 pm EDT

Table of Contents

For more details about the Information Security Office, **please visit our website**!

The best way to deal with disruptive behavior in a Zoom meeting is to prevent it from happening in the first place. Here are Wharton's guidelines to secure your Zoom meetings and deal with disruptions in an active Zoom meeting.

Penn Zoom Default Settings

The following security features have been set on your Penn Zoom account:

- Passcodes are required for all new meetings (does not apply to Personal Meetings)
- The host is the only person who can screen share
- Shared screens may be annotated by all meeting members.
- Participants who have been removed from the meeting will not be allowed to rejoin the meeting

Top

General Guidelines

Zoom bombing, wherein participants join Zoom meetings to cause a disruption, can derail any meeting. There are some things that you can do to thwart potential Zoom bombers before they even have the chance to enter your meeting.

If you need assistance configuring your Zoom settings, **we highly recommend** you reach out to your **Wharton Computing Representative**.

• Do Not Post Meeting Information Publicly

Only share your Zoom meeting details (link, passcode, and ID) with invited participants. Avoid posting them on publicly accessible websites. Canvas course sites are safe since they are only accessible to authorized users.

• Avoid Using Your Personal Meeting ID (PMI)

Your Personal Meeting ID is permanent and always uses the same login information, which makes it convenient but less secure. **Instead, create unique Zoom meetings for classes or work sessions.**

- Enable Waiting Room

Set up a waiting room for every meeting. This allows you to screen participants before admitting them, ensuring that only the right people gain entry. To enable the Waiting Room for a Zoom meeting as it is taking place (and you are the host/co-host of). For more details, **see instructions here**.

- Allow Penn Authenticated Users Only

For added protection, require participants to be logged in with their Zoom account before joining. You can limit it to Penn users only or anyone with a Zoom account. Specific exceptions can be added per meeting.

> **Note**: Penn users only is the default and recommended authentication setting. You can change this by clicking **Edit** next to "Sign in to Zoom" under "Meetings & Webinar Authentication Options" and checking the default box.

You can require authentication on a per-meeting basis or by default for all meetings. For more details, **see instructions here**.

Top

During Your Meeting

Despite following all of our recommendations, disruptions could occur in a Zoom meeting in which you're the host (or co-host). There are a few Zoom tools that make it easy to deal with a disruptive participant quickly:

- Remove Participant

Remove disruptive attendees who will not be able to rejoin. For more details, **see instructions here**.

- Lock Meeting

Prevent new participants from joining once everyone is present. For more details, **see instructions here**.

- Suspend All Activities

This turns off cameras, microphones, screen sharing, and chat, giving you time to assess and remove disruptive individuals. For more details, **see instructions here**.

Top

After Your Meeting

If any of your Zoom meetings are disrupted besides using the features above, report the incident to the Wharton Information Security Office (security@wharton.upenn.edu). They can engage additional resources, if needed, and offer any help you may require.

Top

Questions?

Contact your Wharton Computing Representative or the Wharton Information Security Office for more information.