



## Zoombombing Prevention Tips

As we have quickly moved into the world of total online collaboration, Zoom has emerged as one of the most popular and useful tools to bring our staff and community together. It is easy to learn and use, offers high-quality audio and video, and works on almost any device.

For those of you looking to connect in a synchronized fashion with your class or with a group of students, Zoom is a platform that can serve this purpose. You can use your neshaminy.org email to open a free account that does not have the typical time/person restrictions of the free program.

ISSUE: This newfound popularity has also led to a rise in “Zoombombing,” basically described as the infiltration of unwanted participants and content into Zoom conferences.

***Please read the tips below, adjust your default meeting settings, and take the time to get to know the features of this program before scheduling your next meeting.*** These measures won't prevent every challenge; it is still up to the meeting host to monitor participants and be ready to remove any unwanted users.

### Step-by-Step: Default Settings

Log into your Zoom account on a web browser: [www.zoom.us](http://www.zoom.us). (These same settings in the order below will not be visible on the Zoom app.) The settings can be found by choosing “Settings” on the left side of the dashboard page:

The screenshot shows the Zoom web dashboard. The top navigation bar includes the Zoom logo, links for SOLUTIONS, PLANS & PRICING, CONTACT SALES, SCHEDULE A MEETING, JOIN A MEETING, and HOST A MEETING. A green banner at the top contains an important notice about the Waiting Room feature. The left sidebar has a 'PERSONAL' section with links for Profile, Meetings, Webinars, and Settings (circled in red). Below 'PERSONAL' is an 'ADMIN' section with links for User Management, Room Management, Account Management, and Advanced. The main content area shows the 'Meeting' settings page, with the 'Meeting' sub-menu also circled in red. The settings include: 'Schedule Meeting', 'Host video' (toggle off), 'Participants video' (toggle off), 'Audio Type' (radio buttons for Telephone and Computer Audio, with Telephone and Computer Audio selected), and 'Join before host' (toggle off). A 'Help' button is visible in the bottom right corner.

You can then scroll through all the settings in the center column. Check the default meeting settings below and change them if necessary (not every setting is listed here, only those needed to ensure meeting security). The ones that are **highlighted** are of extra importance, though all of these should be followed. They are listed in the order they appear in the settings column:

## SCHEDULE MEETING

---

- Host Video **OFF (disables your video until you are ready)**
- Participants Video **OFF (disables participant video until they are ready)**
- **Join before Host OFF (disables participants starting the meeting without the host)**
- Only authenticated users can join meetings from Web Client **ON**
- The following three settings may be locked by admin but should be set to **ON**:
  - Require a password when scheduling new meetings
  - Require a password for instant meetings
  - Require a password for Personal Meeting ID (PMI)
- Embed password in meeting link for one-click join: **ON**
- Require password for participants joining by phone (locked by admin): **ON**
- Mute Participants on Entry: **ON (disables audio until participants un-mute themselves)**

## IN MEETING

---

- Chat: **OFF (disables chat function)**
- **Private chat: OFF (disables private chats among participants)**
- File transfer: **OFF (participants cannot upload files)**
- **Screen Sharing** settings:
  - Who can share? **HOST ONLY (THIS ONE IS IMPORTANT!)**
  - Who can start sharing when someone else is sharing? **HOST ONLY**
- Disable desktop/screen share for users: **OFF**
- Annotation: **OFF**
- Whiteboard: **OFF**
- Remote control: **OFF**
- Nonverbal feedback: **OFF**
- Allow removed participants to rejoin: **OFF**

## IN MEETING (ADVANCED)

---

- **Allow participants to rename themselves: OFF**
- Far end camera control: **OFF**
- **Waiting room: ON (Host must allow participants into the meeting)**
- Show a "join from your browser" link: **ON** (this allows participants who cannot download the Zoom program to participate)

## EMAIL NOTIFICATION

---

- When attendees join meeting before host: **ON**
- When a meeting is cancelled: **ON**

# Hosting Safety Tips

## Generate a unique meeting ID every time

If you have a recurring meeting, generate a new meeting ID every session. It's less convenient, but will limit the chance that an ID is misused.

## Don't share the meeting ID publicly

Use email, texts, or other direct contact to share the meeting ID directly with invited participants. Do not share on social media or any other platform visible to non-participants.

## Use the Waiting Room

The Waiting Room function allows you to see and control who is entering your meeting. Unknown participants can be left out.

## Require real first & last names

Do not allow meeting participants to make-up screen names. This is another way to ensure that the right participants are entering your meeting.

## Lock your meeting

Once everybody has arrived for your meeting, click Manage Participants. On the Participants tab, click **More** at the bottom right. There, you can lock your meeting to prevent any additional participants joining.

