Preventive Measures

1. **Use a Waiting Room**:
   - Enable the **waiting room** feature in Zoom, which allows the host to control when participants join the meeting. You can screen participants and admit them individually, ensuring that only invited attendees are allowed to join.
2. **Require a Meeting Password**:
   - Set up a **password** for your Zoom meetings. Only those with the password can enter the meeting, which makes it harder for Zoombombers to get in. Avoid sending the password in the same place as the meeting link.
3. **Only Share the Link with Trusted People**:
   - Share the meeting invite link only with trusted participants. Avoid posting the meeting link on public platforms or social media.
4. **Disable "Join Before Host"**:
   - Turn off the "Join Before Host" setting to prevent participants from entering the meeting before the host. This prevents Zoombombers from accessing the meeting if the host isn't already present.
5. **Lock the Meeting Once All Attendees Have Arrived**:
   - Once everyone has joined the meeting, **lock** the meeting so no new participants can join. This is done via the **Participants** menu by selecting **Lock Meeting**.
6. **Control Screen Sharing**:
   - Limit **screen sharing** privileges to the host only, or specify that only certain participants can share their screen. This helps prevent Zoombombers from hijacking your screen during the meeting.
7. **Enable Two-Factor Authentication (2FA)**:
   - Implement **2FA** for all participants, particularly if you are hosting sensitive or high-stakes meetings. This adds an extra layer of security.
8. **Update Zoom Software Regularly**:
   - Ensure you are using the latest version of Zoom, as updates often include security fixes to protect against new threats, including Zoombombing.