Here are some tips from the FBI, Zoom and other experts to prevent Zoombombing:

- Keep meetings and classrooms private. Do this by requiring a meeting password. Additionally, the “Waiting Room” feature can help hosts control who enters.
- Do not share invites to Zoom meetings on social media. Instead, send the meeting password directly to attendees.
- Use a random meeting ID, so it can’t be shared multiple times. According to Zoom’s website, this is safer than using a “Personal Meeting ID."
- Change screen sharing settings to “Only Host,” so no one but the host can control the screen. The host can also mute participants in their settings.
- Lock a Zoom session that has already begun so no one else can join. Do this by clicking “Participants” in the bottom of a Zoom window, then clicking “Lock Meeting.”
- Remove participants by hovering over their name in the Participants menu, and clicking the “Remove” option. The removed participant will not be allowed back in, according to Zoom’s website.
- The FBI advises users to make sure they have the most updated version of Zoom’s software. A recent security update added default passwords and disabled the ability to scan for meetings to join.