Zoom can be a great collaborative tool, but that also means that hosts of meetings need to be particularly careful about who and what they're allowing others to access while in a synchronous environment..

To help keep your calls safe and secure from unwanted intrusions, try the following:

1. **Utilize Waiting Rooms**
   If your meeting is of a manageable size, you could enable Waiting Rooms. This would send all guests to a temporary personal "waiting room", where they would have to be individually approved by the host before entering the actual meeting call. This setting can be enabled in the Meeting settings on the website.

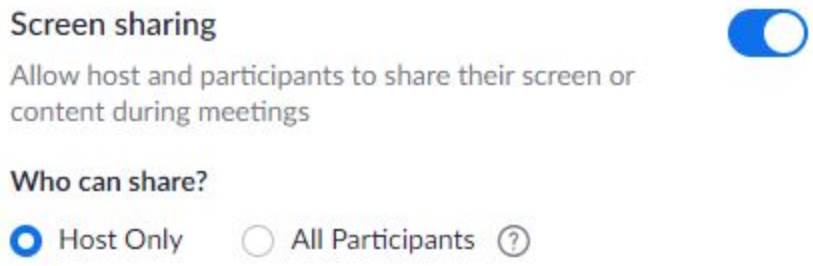
2. **Lock the Meeting**
   Once your class is in session, you can choose to lock your meeting by clicking on the Manage Participants tab in your toolbar. You'll see this option under the drop down menu titles "More", in the bottom right corner.

   Just be sure you have a way for students to contact you. They'll be unable to get in, even with a password, while the meeting is locked.

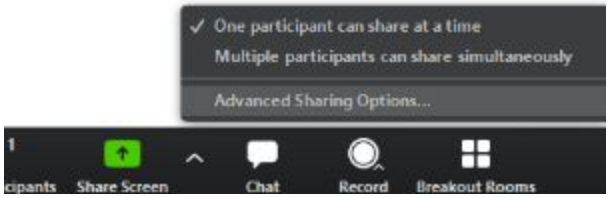
3. **Be mindful of where you share links to your meetings.**
   While links to meetings can be a convenient way to grant your students access to a call, remember to be careful of where you're sharing them. Tweeting out a link or making a general post with it on Facebook might give your meeting a lot more exposure than you originally intended.

4. **Try not to use your Personal Meeting ID for classes**
   Your Personal Meeting ID (PMI) is a meeting that is specifically assigned to you, and one that you can return to for a variety of purposes. Given that, it's generally more secure to use randomly assigned Meeting IDs when meeting with students.

5. **Limit who can share content**
   Unless you plan on letting students share their screen, it may be beneficial to disable all non-host screen sharing. This can be done on the Setting tab on zoom.us, under your account.



   This can also be toggled as an option **during** a call by clicking on the upward arrow near the Share Screen button and clicking on "Advanced Sharing Options…"



6. **Disable Annotations and File Transfer**
   Annotations are a collaborative way for guests and hosts to interact with shared content, but they can also be disruptive or inappropriate if abused. If you're not planning on using them, they can be disabled in your settings on zoom.us.

   Same goes for File Transfer- if you don't need guests to share files, you can toggle that to off to prevent the possibility of inappropriate or disruptive file content entering the chat.

7. **Disable Private Chat**
   While students certainly have other ways to message each other, you can ensure that guests aren't harassing each other directly by closing the private chat. This too can be done in Meeting Settings online.

8. **Disable Join Before Host**
   To ensure that you as a host can actively monitor everything that happens in a meeting, you can disable the ability for guests to join the call before the host.

9. **Only record when necessary**
   While Zoom does have a built in recording option, it is important that you be up front about when you plan on using it. Be advised that it is not recommended to record a synchronous meeting unless absolutely necessary.

10. **Actively manage participants**
    If you have a particularly disruptive participant, remember that as a host you have privileges to remove them from the meeting, mute them, and disable their video. Note that in an emergency, you have the ability to Mute/Unmute All in the Participants tab during a call.

You can see more ways to keep your meeting safe on the official Zoom blog.
As always, please reach out to the Learning Technologies Team at ltt@truman.edu for any questions or concerns!