PROUDLY PRODUCED BY
MOREHEAD PLANETARIUM + SCIENCE CENTER
The University of North Carolina at Chapel Hill

**Security Tips for Zoom Meetings & Webinars**

Here are a few recommendations and considerations from the NCSciFest Team to help secure your Zoom Meetings and Webinars and prevent unwanted participation (sometimes called "Zoombombing").

**Zoom Meetings**

- **Waiting Room:** One of the simplest and easiest ways to prevent unwelcome people joining your meetings is to enable "Waiting room" in your account settings. Turn this on to place everyone joining the meeting into a waiting room, and the host approves each person (or clicks approve all) before they can enter the actual meeting room. This can also be set for "Guests Only" so that people logged in to their Zoom accounts can bypass the waiting room. You can also customize the waiting room with a message and/or logo.
- **Meeting ID:**
    - Consider whether you need to share the link publicly – it may be better to require people to register with their email address and then send them the Zoom link.
    - Don't use your personal meeting ID: Personal meeting rooms are good for quick meetings with trusted people, but it's not a good idea to share that link publicly.
- **Check other settings:** Some of these are only accessible by logging in to your Zoom account online, while others can be adjusted on the fly.
    - Turn off "Allow removed participants to rejoin"
    - Set "Screen Sharing" to "Host only"
    - Determine chat needs – consider setting "Participant can chat with:" to "No One" or "Host Only"
    - Consider turning on "Nonverbal feedback" to provide participants with some limited options to interact
    - Turn off "Annotation" and "Whiteboard" unless needed for your meeting
    - Consider muting participants on entry and whether to allow them to unmute themselves
    - Consider unchecking "Allow Participants to Rename Themselves"
- **Use a trusted co-host:** If possible, assign a dedicated person to "co-host" your meeting. This helper can admit people from the waiting room, remove any harassers, transfer host status to anyone needing to share screens, and mute or unmute participants.
- **Passwords:** Passwords can be used to limit access to a meeting room but remember that anyone with the password can share it with others without your permission.

**Zoom Webinars**

- **Chat:** Ensure that participants are only able to send chats to "All Panelists." If you don't need chat at all, consider changing the setting to "No One."
- **Q&A:** Make sure that Q&A is set so attendees can only see "answered" questions. Also, be sure to uncheck the box to allow anonymous questions. This lets you identify and remove people who abuse the system.
- **Use a dedicated co-host:** Be sure to have someone behind the scenes who can mute and unmute panelists, start and stop screen-sharing, remove harassers, lower hands, allow participants to turn on microphones as needed, dismiss questions or mark as answered, and respond to any technical issues.
- **Registration:** Consider requiring registration. This requires people to submit their name, email address, and any other fields you'd like to require in order to receive the link to join via email. Turning off automatic approval allows you to control who receives the link after signing up.

**Learn More**

Zoom's blog features a handy guide that covers some of these topics:
https://blog.zoom.us/wordpress/2020/03/20/keep-uninvited-guests-out-of-your-zoom-event/