LCOM Technology Services
Zoom Meeting Best Practices

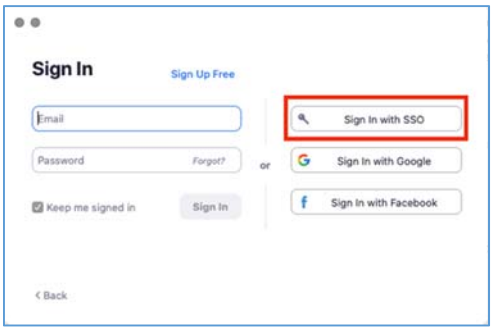
Protect your Zoom meeting

We've assembled this list of best practices that will add a layer of security to your Zoom meeting and protect against interruptions during your meeting.

1. Please use your LCOM – licensed Zoom account when conducting UVM business. Authenticate with your LCOM username and password (this would be your first.last@med.uvm.edu account).

   To get started, visit https://uvmcom.zoom.us and select Sign In.

   If you have the Zoom App on your computer or device, open the app and use "Sign in with SSO" button. (See image at right). In the Your company domain field, enter UVMCOM.



2. When scheduling a meeting, use an **automatically generated meeting ID** rather than your personal meeting ID.

3. Require participant authentication to join a meeting (e.g. require participants to have a Zoom account to join the meeting). You can turn this off if you are inviting someone who may not have a Zoom account and require a password instead. See #4 below.

4. Require a password to join meeting**.**

5. Disable file transfers**,** annotation and private chat to prevent distribution of inappropriate or malicious content.

6. Use a waiting room to control when participants join your meeting.

7. Disable the ability for **participants** to rename themselves.

8. Review your account settings; many of the controls mentioned above can be set as a default and adjusted as needed. They can also be changed on a per meeting basis as noted below.

9. Know how to manage participants during a meeting, including:
   a. Removing unwanted participants from a meeting
   b. Not allowing others to share their screen, locking the meeting so that others cannot join the meeting once it begins, and more.
   c. Do not share your **meeting links** or **passwords** publicly (e.g. social media).