zoom SAFETY

Follow these steps to keep your virtual meetings and class sessions on-task:

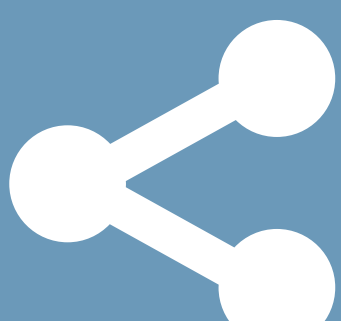
click the icon for more info!

1 AVOID PUBLISHING LINKS

Links to Zoom meetings should not be published on publicly accessible webpages. The standard formatting of the URL makes it an easy target for web crawlers to discover your link and attempt to join your meeting. Send Zoom meeting links through trusted communication channels such as email, calendar, text, or a class website that requires user authentication.

Events that require a public distribution of a Zoom URL should be moderated and secured with additional controls.

2 RESTRICT SHARING SETTINGS



Meetings in Zoom allow all participants to share content by default. This could include an unwelcome guest. Change your Zoom meeting preferences so only hosts and co-hosts may share content. You can promote participants to co-hosts by right clicking their name from the Participants window.

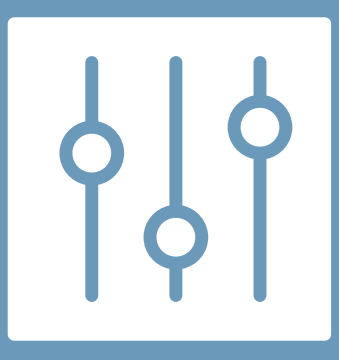
Note: On 3/26/2020 Zoom made this the default setting for education accounts.

3 SCHEDULE INDIVIDUAL ZOOM SESSIONS

Although convienient, recurring meetings share the same meeting ID. Zoom meetings are safest if the meeting ID changes for each scheduled session.

Your Personal Meeting ID (PMI) should only be used for quick, impromptu meetings and should not be shared broadly. The PID can be changed from your account settings at www.zoom.us

4 USE PARTICIPANT CONTROL FEATURES



Is one of your participants breathing into their microphone, causing feedback, or sharing their webcam at an inopportune time? You have the power to mute, disable video, or even remove an attendee! Simply right click a participant to perform these and other functions.

Assistance with Zoom settings and running a Zoom session is available from your college IT department.

Maine Community College System