From: Office of the Provost
To: KU Lawrence All Staff, Faculty and Affiliates; All KU Lawrence and Edwards Students
Subject: Zoom Meeting Security Best Practices
Date: Friday, April 10, 2020 3:39:43 PM

KU | OFFICE OF THE PROVOST

Sent on behalf of Mary Walsh, Chief Information Officer, and Chris Brown, Vice Provost for Faculty Development

Zoom Meeting Security Best Practices

Jayhawks,

Zoom, an online video meeting tool of choice during the coronavirus crisis, has been in the news recently for security vulnerabilities that allow uninvited participants to join and disrupt meetings. As part of its response, Zoom recently disabled all educational customers' screen sharing by default. KU IT is making additional changes on Tuesday, April 14 to ensure your Zoom meetings are more secure:

- New meetings will be configured to require a password by default. (Note: Meeting attendees joining by phone will not be required to use a password.)
- Caller ID will be partially masked for meeting attendees joining by phone.

Some settings remain under user control, and KU IT recommends you do the following when you create a meeting:

- **Always set up meetings at kansas.zoom.us** instead of through a personal account. This ensures the meeting is organized behind KU log in and has multi-factor authentication protection.
- **Never post the meeting link, meeting ID or password in a public place.** In other words, do not post meeting IDs and/or passwords on social media or a website, such as in an online syllabus, or in a place this is not protected by KU log in. KU IT Security recommends sharing meeting information only through Blackboard or KU email.
- **Generate meeting IDs automatically.** This generates a unique meeting ID, creating a more secure environment for each meeting you

host. Avoid using your personal meeting ID because anyone who has your personal meeting ID link can join any meeting that also uses that link. I.e., a malicious actor could enter any meeting you create.

- **Disable "Join before host."** This will prevent participants from launching the meeting.
- **Select "Mute participants on entry."** Participants can turn on their microphones once they are in the meeting.
- **Consider disabling annotation.** When sharing your screen, you will need to decide whether participants will be able to annotate on the shared screen. KU IT recommends disabling attendee annotation unless you are sure all participants present are known.

NOTE:

- **Meetings set up before these changes' implementation date are not covered and will need to be updated manually.**
- Zoom has implemented a "Security" toolbar button that is viewable once a meeting has begun. From the button you can lock the meeting to new participants, enable the waiting room and toggle participants' ability to chat, screen share and rename themselves.

Public meetings

Public Zoom meetings are discouraged, but if you must make your meeting public, please require registration. You will see registration as an option near the top of the initial meeting settings, just below "Time Zone." Registration provides you with participant information before the participant is given the meeting URL.

Note:

- Requiring registration will prompt you to choose automatic or manual approval. Manual approval will allow the organizer to more thoroughly screen meeting participants.
- Passwords will still be required for public meetings.

Resources

Please review this Zoom help article for more information on meeting settings.

KU IT has created the following handouts to help you orient with Zoom:

- Using Zoom at KU – Quick Start Guide.
- Using Zoom at KU – Instructors.

- Using Zoom at KU – Students.

KU IT staff are ready to assist if you need help with Zoom or any other supported application. Call 785-864-8080 or email itcsc@ku.edu.

Thank you,

Mary Walsh and Chris Brown

Mary Walsh
Chief Information Officer

J. Christopher Brown, Ph.D.
Vice Provost for Faculty Development
Professor, Department of Geography and Atmospheric Science
Environmental Studies Program