Key steps to prevent Zoombombing and secure your meetings

Michele Norin <cio@rutgers.edu>

Thu 2/18/2021 4:07 PM

To: INFO_FS_ALLCAMPUSES@RAMS.RUTGERS.EDU <INFO_FS_ALLCAMPUSES@RAMS.RUTGERS.EDU>

Members of the Rutgers Community:

Our community values frequent collaboration and vibrant conversation in an environment of inclusivity and respect. Much of this now happens virtually. To nurture and protect the Rutgers community in this virtual environment, and in light of recent Zoombombing incidents at Rutgers and other institutions, we want to share best practices to help ensure your web conferencing meetings are secure.

To help prevent unwanted guests in your Zoom, Webex, or other web conferencing meetings, we strongly advise that you review the resources at our web conferencing security webpage, including key tips to avoid Zoombombing and unwanted meeting guests. These resources include information on how to lock your session, only allow Rutgers users to join, disable chat capabilities, and more.

Additionally, you should avoid sharing meeting links on social media, webpages, or other public forums. By sharing your meeting links publicly, you are increasing the risk of Zoombombing. To promote your events, please review this guidance for sharing your Zoom meeting or webinar securely.

If you have questions on how to avoid Zoombombing or the use of web conferencing systems at Rutgers, please contact the Office of Information Technology Help Desk.

Thank you,

Michele Norin
Senior Vice President and Chief Information Officer