As universities across the world are moving online, the prevalence of “Zoom bombing”—when individuals disrupt a Zoom meeting—has increased. Unfortunately, the University of Delaware community has experienced such disruptions this week. These disruptions can be upsetting and offensive, and they violate UD policies. New requirements are being implemented to immediately address these disruptions.

To protect the learning experience of UD students from these types of intrusions, UD Information Technologies (UDIT) is activating new global Zoom controls. These new controls will require action by faculty using Zoom in classes.

Faculty must use the following settings when scheduling new meetings and must update any existing meetings already scheduled in order to prevent future disruptions.

At their next class meeting, faculty may wish to share that students who are found participating in or enabling Zoom bombings will be referred to the Office of Student Conduct. Enabling Zoom bombing includes the sharing of Zoom meeting IDs and other relevant class information outside of your class. This is a violation of the University of Delaware's Responsible Use of Computing Policy and potentially other policies at UD. If a student is found responsible for violating policies, they will be sanctioned appropriately.

If you have graduate teaching assistants who are scheduling synchronous Zoom meetings for their sections, please be sure to share this message with them as well.

If you are teaching live via Zoom for UD students

Ensure the “Only authenticated users can join” setting is enabled to best protect your meeting. Students will need to be logged in to the Zoom application before they can join. Any meeting attendees who are not logged in to Zoom with UD credentials will not be able to join. If you are enabling this setting, inform your students that they will need to log in to the Zoom application to access the meeting.

If your meeting includes non-UD attendees

Ensure the “Only authenticated users can join” setting is **disabled** for these meetings. Instead, you can protect such meetings by:

- Enabling the waiting room feature.
- Setting a meeting password. Share this password with your invited attendees via a message separate from the meeting invitation.

These features are an effective protection against uninvited external individuals in your Zoom meetings.

What to do if you encounter a Zoom bombing

- The meeting host can use the Manage Participants window to remove disruptive participants from a meeting. Removed participants cannot re-enter the meeting.
- If you have too many unwanted participants to manage, consider ending your meeting.
- Avoid publishing recordings of classes with incidents. UDIT will follow up with faculty regarding the need to publish when a Zoom bombing report is made.

Report all Zoom bombing incidents to IT Security by emailing askit@udel.edu or submitting this form.

Visit UDIT's Zoom security page for detailed steps for the above instructions and for additional information about meeting controls.

UDIT recognizes that a significant amount of work went into moving your courses online and that these disruptions are stressful to you and to your students. Although these changes require additional action on your part, they will better protect the learning experience of all students and the UD community. As always, UDIT is here to support your efforts.

For support, questions or concerns contact UD Information Technologies.

Sharon P. Pitt
Vice President of IT & CIO
UD Information Technologies