March 23, 2020

As Zoom use increases, some disruptive individuals are trying Zoom-bombing [2], or gate-crashing Zoom meetings. Duke provides recommendations on Zoom settings [3] to protect the privacy and security of your meetings.

Among the recommendations:

- Avoid sharing your meeting link on public channels.
- Use a randomly generated meeting ID instead of your Personal Meeting ID.
- Restrict participant options when setting up the meeting to manage screen sharing and participant activity. The Waiting Room [4] feature, for example, allows hosts to control who enters the meeting.

For more on privacy considerations when using Zoom, visit https://scholarworks.duke.edu/privacy/ [5].

Additional recommendations are available on Zoom’s blog [6].

Source URL: https://security.duke.edu/news-alerts/protect-your-zoom-meetings

Links
[1] https://security.duke.edu/news-alerts/protect-your-zoom-meetings
[5] https://scholarworks.duke.edu/privacy/