Protect your Zoom meetings [1]

April 2, 2020

Zoom has announced new plans to address security and privacy concerns [2] and has released updated tools and resources to help users understand how best to protect their meetings.

In addition to releasing fixes to address several issues identified by security researchers, Zoom clarified how encryption is implemented in this blog post [3]. Over the next 90 days, Zoom is increasing its efforts to identify and proactively fix issues, including:

- Enacting a feature freeze across the platform so engineering can focus on security and privacy.
- Creating an advisory council made up of chief information security officers from various industries.
- Conducting a third-party security review of code and penetration tests for the platform.
- Weekly security/privacy webinar updates at 10pm PT.

Duke’s IT security offices are continuing to monitor these issues and are working directly with Zoom to address any concerns that arise. Duke faculty, staff and students are encouraged to follow the Office of Information Technology’s recommendations on Zoom settings [4] to protect the privacy and security of meetings. Among the suggestions:

- 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 [5] feature, for example, allows hosts to control who enters the meeting.

Additional Zoom resources for higher education include best practices for:

- Preventing Zoom vandalism [6]
- Securing virtual classrooms [7]

For more on privacy considerations when using Zoom, visit https://scholarworks.duke.edu/privacy/ [8].

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