April 27, 2020

With the recent expansion of Zoom use, Duke’s IT Security Office has taken steps to further examine our relationship with Zoom to address concerns about the platform’s privacy and security. Below are the mitigations in place for Duke Zoom users:

- **Zoom vandalism.** Duke’s Office of Information Technology has published guidance on settings to protect Zoom sessions [2]. Using passwords and following the recommended settings will dramatically reduce the possibility of Zoom vandalism, also known as "Zoom bombing." Meeting hosts should report all incidents of Zoom vandalism using the Report a Participant to Zoom [3] option, as well as notifying security@duke.edu [4]. Zoom also has set specific sharing settings for Education accounts [5].

- **Zoom and data privacy.** Duke’s contract with Zoom includes our standard security and privacy terms, including a Business Associates’ Agreement, to protect Duke’s confidential data. The terms of service are available on the OIT website [6].

- **Zoom’s security controls.** Duke’s IT security offices remain committed to the safety and security of the Duke community and continue to test for and monitor any security issues reported. We have been encouraged by Zoom’s quick response to issues so far:
  - Zoom fixed a privacy concern with the iOS client that made use of the Facebook SDK for development. (No customer content was ever sent to Zoom/Facebook over this SDK.)
  - Zoom fixed security issues identified in Windows and Macs within 24 hours of the issues being reported.
  - Zoom has clarified the details of how it handles encryption [7] to address concerns.

Zoom continues to focus on its security posture. Regular updates are posted: https://zoom.us/security [8].

Duke will continue to test for and work with Zoom to address any issues.
April 2, 2020: How to protect your Zoom meetings

Zoom has announced new plans to address security and privacy concerns [9] 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 [10]. 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 [2] 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 [11] feature, for example, allows hosts to control who enters the meeting.

Additional Zoom resources for higher education include best practices for:

- Preventing Zoom vandalism [12]
- Securing virtual classrooms [13]

For more on privacy considerations when using Zoom, visit https://scholarworks.duke.edu/privacy/ [14].

Source URL: https://security.duke.edu/news-alerts/zoom-security-and-privacy

Links
[3] https://support.zoom.us/hc/en-us/articles/360042791091#h_118b55c7-b13f-41b9-90cc-e003436663bc
[4] mailto:security@duke.edu
[8] https://zoom.us/security
[9] https://blog.zoom.us/wordpress/2020/04/01/a-message-to-our-users/
[12] https://blog.zoom.us/wordpress/2020/03/20/keep-the-party-crashers-from-crashing-your-zoom-event/
[14] https://scholarworks.duke.edu/privacy/