

Zoom: Risk vs. Reward

By Angelo Comeaux and Kenneth Chung

In a day and age where we are all looking for a convenient way to interact with each other, Zoom has really come in to save the day. Schools, businesses, government, yoga classes, happy hours, and birthday parties all swarmed to Zoom as the quarantine began and we began to social distance. Zoom reported that its usage grew from just 10 million users last December to 300 million users by June. We were all so desperate to re-engage in social activities that many of us decided to use the platform without considering the potential risks.

There have been complaints about security and privacy issues that have caused many agencies to stop using the platform at some time during this year. Zoombombing, one of the biggest complaints about the platform, was not an issue with the platform itself; It was an issue resulting from users sharing meeting IDs publicly and not enabling security that was already available. When the DOE banned Zoom for online classes in April, most teachers were devastated; Google and Microsoft just didn't do the job as well. Zoom was willing to partner with the DOE to "fix" the issues - making security settings a default setting and using the enterprise version, requiring all users to join with DOE credentials. There have also been complaints that Zoom data can be hacked when streaming, but that just means it's only as safe as any other online activities we engage in - all data sent over the internet can be captured. Zoom may come under more scrutiny with highly-sensitive data, but it's good enough for everyday use with a little training on how to follow best practices.

The internet is built with inherent vulnerabilities. Because of this fact, it is up to producers and consumers on the internet to create and facilitate digital communication that is safe and secure. Zoom, as the owner of a commercial product, has a responsibility to the users of its product to fairly represent its safety and disclose what it does with the sensitive personal information of its users. In many ways and on multiple occasions Zoom has failed in this responsibility and they should not be quickly trusted to act in the best interest of their users. In 2019, an independent researcher discovered that Zoom's Macintosh application was hackable to such a degree that any malicious actor could gain access to your webcam without your knowledge. They've reportedly sent information to Facebook about users' Zoom habits even if the user didn't have a Facebook account. This prompted a lawsuit. The platform was also leaking personal email addresses at one point. A more egregious offense was that they falsely claimed that their service was end-to-end encrypted when in fact it was not.

Now a new company, Class EDU, is looking to push Zoom further into the education space. Their new education platform, Class for Zoom, will have tools that allow teachers to monitor students' computers. They can gather intel on whether a student has Zoom as the

primary app in use or not. Teachers can monitor a student's desktop during an exam. The new platform with its added "features" is sure to bring concerns of privacy and added threats and vulnerabilities along with it.

The digital learning space will continue to grow, regardless of the providers present in the space. For virtual learning to be successful, good tools need to exist and many aspects of Zooms latest developments lend to that, but the key point of the argument against Zoom is that Zoom has been misleading in its claims and actions on several fronts with seemingly little to no accountability, putting its users in harm's way in the process.

Sources:

"Zoom at Your Own Risk" a short synopsis of Zooms security issues

- <https://techcrunch.com/2020/03/31/zoom-at-your-own-risk/>

Zoom banned in NYC schools

- <https://techcrunch.com/2020/04/05/zoom-new-york-city-schools/>

Is Zoom safe for schools?

- <https://elevate.explo.org/zoom-is-it-safe-for-schools/>

Zoom unbanned in NYC schools

- <https://ny.chalkbeat.org/2020/5/6/21249689/nyc-schools-education-zoom-ban-reversed>

Zoom is trying its best

- <https://www.forbes.com/sites/kateoflahertyuk/2020/06/05/zooms-security-nightmare-just-got-worse-but-heres-the-reality/>
- <https://www.cnet.com/news/zoom-security-issues-zoom-buys-security-company-aims-for-end-to-end-encryption/>

Class for Zoom preview

- <https://techcrunch.com/2020/09/23/class-for-zoom-earliest-investors-are-betting-millions/>

A Timeline of Zoom Issues (and fixes)

- <https://www.tomsguide.com/news/zoom-security-privacy-woes>

Zoom still vulnerable to inside mischief

- <https://www.foxnews.com/us/nyc-remote-learning-zoom-hack-appears-to-be-inside-job-officials-say>