Should you still use Zoom?

Zoom has been in the news lately. And many people are asking, "Should you still use Zoom?"

I am not a cyber security expert. In fact, I have been advised by our network consultants that we should be using Microsoft Teams instead of Zoom. While Microsoft Teams IS much more secure than Zoom, the real reason for their recommending Teams over Zoom is because of the robust features of Teams over and above its use as a video meeting platform. Over the next few days, I will cover Microsoft Teams so you can decide for yourself. In the meantime, here are some of Zooms reported security weaknesses. The following includes excerpts from online articles on the subject plus my interpretation.

Questionable routing:

> a) The apple app was sharing info with Facebook. That vulnerability was removed from the app on March 27, 2020.
>
> b) Due to an error Zoom routed traffic SOME through China - a country known for heavily monitoring traffic. The problem started when Zoom added several new servers to handle explosive, pandemic-related growth. Only a small group of meetings were routed through China AND Zoom has removed all servers it operates in China from its global rotation.

Encryption: It doesn't use top of the line encryption. It is encrypted but it is not the best encryption. This appears to still be an issue. Zoom says better encryption is on its way. They are consulting with experts in the field and hope to have better encryption methodologies in the next 45 days. In the meantime, should you care? You SHOULD care but chances are you aren't a target

> Brian Feldman of the NY Magazine wrote "The documented security flaws of Zoom would require a high level of targeting and precision to fully exploit. This isn’t the sort of lax security that could lead to catastrophic widespread data leakage; it’s the sort of lax security that leaves high-value individual targets vulnerable."
>
> Glenn Fleishman of fastcompany.com writes that on Steven Bellovin’s blog the security guru indicates “What it boils down to is this: Exploiting the lack of true end-to-end encryption in Zoom is quite difficult, since you need access to both the per-meeting encryption key and the traffic.” That means governments and very determined parties might be able to exploit this potential weakness. But not casual hackers.

Zoombombing:

- Bad actors, who guessed room IDs manually or by using automated scripts, were able to gain access to meeting rooms. They were verbally interrupting meetings and sharing offensive content. Securing your room with a password, enabling the waiting room, locking meetings once in session and disabling the annotation feature, custom backgrounds and screen sharing for participants renders those attackers powerless now. (Meeting passwords and the Waiting Room are enabled by default for all Zoom meetings. All other security settings have been organized under the easy-to-find security tab at the bottom of the screen.)
- Kids were also changing their screen names after joining the meeting to offensive or just silly words. Hosts can now prevent meeting attendees from changing their name.

- Another vulnerability stemmed from people sharing Zoom meeting screen shots on social media. Those images were revealing room meeting IDs which allowed malicious individuals into meetings that were not password protected. Meeting IDs are no longer visible on-screen.
- Participants can still share links and passwords with their friends. When it comes to the classroom setting, setting consequences for sharing private meeting information should be considered. However, use of the Waiting Room feature can help corral people. In a large meeting, checking participants against an attendance list may be helpful.
- AND, for goodness sake, NEVER use your personal room ID. While personal rooms are now also covered by a password, the password is not changeable. Your personal room ID is basically one long meeting anyone you've ever given access could rejoin.

What's the bottom line?

Feldman also wrote "If you work for a government entity or a multinational corporation, or you handle sensitive information like medical or financial data, maybe take a look at some of Zoom's competitors - Google and Microsoft...." "But if you're using Zoom's most recently updated software and you have basic privacy features enabled,..." such as password-protecting your meetings and utilize the waiting room feature, "...you can probably rest easy."

Fleishman also wrote "Human-rights activists, companies engaged with sensitive intellectual property, public officials discussing critical points of security and public safety, and those in legal, medical, and financial industries who have specific regulatory demands should likely avoid the platform until it implements true end-to-end encryption."

Zoom is committed to fixing their security flaws and have dedicated all staff to the goal over the next 90 days.

Read articles I used in my research here:

https://nymag.com/intelligencer/2020/04/the-zoom-app-has-a-lot-of-security-problems.html
https://www.fastcompany.com/90488717/can-you-trust-zoom
https://www.latimes.com/business/technology/story/2020-04-13/is-zoom-safe-to-use-heres-what-you-need-to-know