Protect against malicious Zoombombing

Over the past few days, I have seen numerous reports from my university and in the popular press about groups organizing to disrupt online meetings with pornographic and/or hate images and threatening language. This morning, an open-access meditation session facilitated by a member of our community was disrupted by such a group.

The United States Federal Bureau of Investigation is investigating these occurrences, but has not yet gotten to the bottom of them. It appears that loosely-banded groups are organizing, targeting particular meetings, sharing meeting information via Instagram postings, and then sharing video captures of the reactions, again on Instagram.

My university offered us some guidance from the FBI that I thought would be useful to share here.

Another option is to use any of a dozen other live meeting platforms. But given the versatility of its features and the current ubiquity of Zoom, it might help for us to share and discuss these recommended practices.

Note that some of us using Zoom cannot make use of *all* these recommendations. For example, one suggestion is to make meetings private and require a meeting password. But if you are hosting an open session for the public, that might inhibit attendance. I guess you’ll want to consider the audience you aim to reach and which prospect poses the greater risk. And use the ones that make sense for you in your context.

At any rate, here are recommendations from the US FBI to our university:

• Do not make meetings or classrooms public: In Zoom, there are two options to make a meeting private:

* require a meeting password or
* use the waiting room feature and control the admittance of guests.

• Do not share Zoom conference links on public social media: Provide the link directly to specific people.

• Manage screen-sharing options:

* In Zoom, change screen sharing to 'Host Only.'
* If you allow participants to screen share, you can specify the participant(s) that you are granting permission to share their screens

·         Using Zoom’s  [Audio signatures](https://www.youtube.com/embed/fYqUoXDqJIw?rel=0&autoplay=1&showinfo=0) protects against unauthorized recording and sharing of Zoom meeting content.

·         Enable/disable a participant or all participants to record

·         Keep your version of Zoom up to date:  In January 2020, Zoom updated their software. In their security update, the teleconference software provider added passwords by default for meetings and disabled the ability to randomly scan for meetings to join.

**F*BI advises zoom-bombing victims to report such incidents via the FBI’s Internet Crime Complaint Center and any direct threats during a video conference hijacking incident at***[***https://tips.fbi.gov/***](https://tips.fbi.gov/)***.***

***Articles and advice:***

[***https://zoom.us/security***](https://zoom.us/security)

Also note:

<https://threatpost.com/zoom-scrutinized-as-security-woes-mount/154305/>

And:

<https://www.computerweekly.com/news/252480806/Coronavirus-Warning-over-surge-in-Zoom-security-incidents>

These are from the New York Times:

<https://www.nytimes.com/2020/04/03/technology/zoom-harassment-abuse-racism-fbi-warning.html?action=click&module=Top%20Stories&pgtype=Homepage>

<https://www.nytimes.com/2020/04/02/technology/zoom-linkedin-data.html?action=click&module=RelatedLinks&pgtype=Article>

Hand to heart,

t.

(Thomas G. Szabo)