BLINN.COMmunications
June 2020
179 Caren Avenue • Worthington • Ohio 43085-2520 • 718.577.1054 (NYC) • 614.785.9359 (Ohio)

Is Zoom's Security Good Enough Yet?

On Mother's Day, the family had a virtual gathering on Zoom. I had used the service once previously for a conference with New York City's Metropolitan Transportation Authority. Then came the alarming news about Zoom's security, or lack of it. Let's see how the company is dealing with the challenge.

Two of the main weak spots were Zoom's technique for generating meeting numbers and not requiring a password to enter the meeting. Another was lack of encryption. As a result, random people could wander into meetings and, if meetings were recorded, they were available online without any protection at all.

Alarming (at least to me) is that some physicians were using Zoom for telemedicine sessions with their patients. There's simply no way that Zoom was complaint with Health Insurance Portability and Accountability Act (HIPAA) privacy guidelines. The *HIPAA Journal*, after previously stating that Zoom was an acceptable telemedicine alternative, now says "Until the security issues with Zoom are resolved, alternative telemedicine solutions should be used."

Zoom is working to provide end-to-end encryption, but only for paid users. It has acquired Keybase, a startup company the specializes in encryption. Until encryption is fully implemented, Zoom is adequate — when used with care — for family meetings, many business meetings, and schools.

It's still questionable for use in healthcare settings where protected health information is shared. The list of what constitutes personal health information is long. In part, it includes patient name, location, birth date, phone numbers, fax numbers, Social Security numbers, medical record numbers, email addresses, biometric identifiers, photos, and a lot more.

Zoom made it possible for us to get together virtually on Mother's Day while maintaining appropriate social distancing.

Addressing Security

On 1 April, Zoom CEO Eric Yuan announced a 90-day plan during which developers would work exclusively on fixing safety and privacy issues. Just before Mother's Day, Zoom made a few changes:

- All meetings must have passwords. Without a password, meetings were accessible to anyone who knew the meeting ID, and many people used the same ID time after time.
- The waiting room function is now turned on by default. People arriving at the meeting will be in the waiting room until the meeting organizer allows them to enter the meeting.
- Meeting participants can no longer share their screen unless the meeting host allows it.

Continued on page 2

Scammers Step In, Too

Scammers are nothing if not inventive, so naturally they're taking advantage of the confusion surrounding Zoom, but not always to steal Zoom credentials.

One scam reported by Abnormal Security works this way:

- The victim receives a message that says they missed a scheduled Zoom meeting, so they should view the recording. At a glance, the message appears legitimate, but looking carefully reveals it as a phony.
- The scam claims the recording will be retained for only 48 hours, so it's important to view it soon.
- The link in the email goes to a phony Microsoft login page that contains the name of the victim's company and a Zoom logo.
- If the victim tries to log in, the scammers receive the Microsoft account user name and password. This would give the crooks access to any information that's stored in the victim's Microsoft account.

Links in messages are an ongoing source of attacks, and users should follow links only when they are absolutely certain that the message was sent from someone they know. Or, better still, log in directly to Zoom to check for recordings of missed meetings. **The best advice always is not to click a link in an email.** Ω

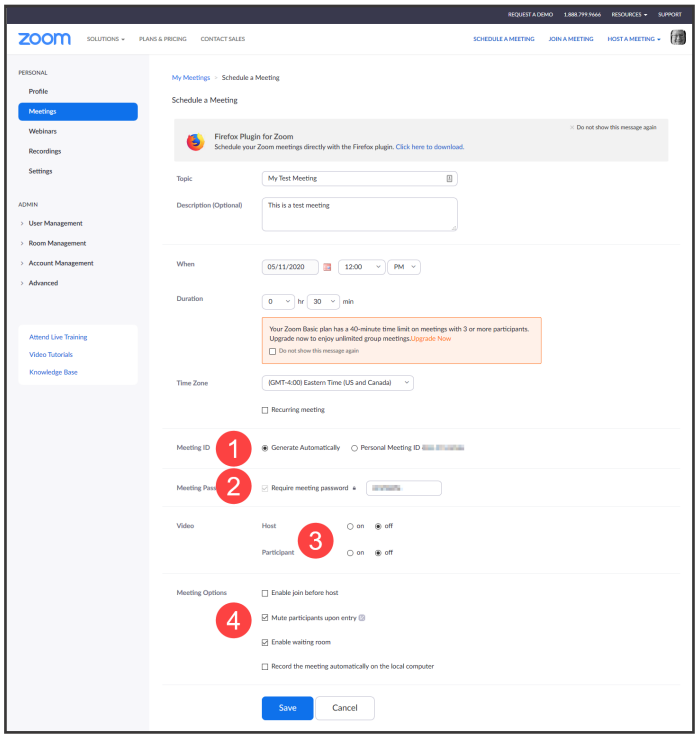
Blinn Communications News (ISSN 2639-5762) is for clients and friends of William Blinn Communications, Worthington, Ohio. Phone 614.785.9359 (Columbus) and 718.577.1054 (NYC). On the Web at www.blinn.com.

These all seem like such good basic security measures that it's odd that they were overlooked until now. Unfortunately, many developers spend a great deal of time on making applications easy to use and fine-tuning the user interface, and choose to look into security for the application only if it catches on. That may be what happened with Zoom.

The company is now in a race with competing providers of online meeting technologies, and some large companies have set internal policies that forbid the use of Zoom for company meetings. The revised functions and additional work on security may allow Zoom to win back some of those paying customers because Zoom has developed a system that's extremely easy to use.

Zoom responded quickly, but a couple of big competitors — Microsoft and Google — also responded quickly by adding features that Zoom users like to their applications. Both have added a feature that looks a lot like Zoom's popular grid view and Microsoft added the ability for users to add custom backgrounds to their images.

Zoom is reminding users to update client applications to version 5.0 before the end of May. Any meeting participants with earlier versions "will receive a forced upgrade when trying to join meetings."



(1) Use Zoom's meeting ID, (2) choose a strong password, turn off both (3) host and participant cameras, and (4) keep participants out of the meeting room until the host arrives.

Making Zoom Safer

When you set up a meeting, it's important to observe several best practices that will improve safety and security.

You can use an (1) existing meeting ID, make up a meeting ID, or let Zoom choose one for you. Let Zoom do it. People are predictable, and allowing the system to create the ID eliminates that danger. The meeting password option (2) can no longer be disabled. If you don't like the password Zoom recommends, you can create your own. Only those who have the password can either enter the meeting or get to the waiting room.

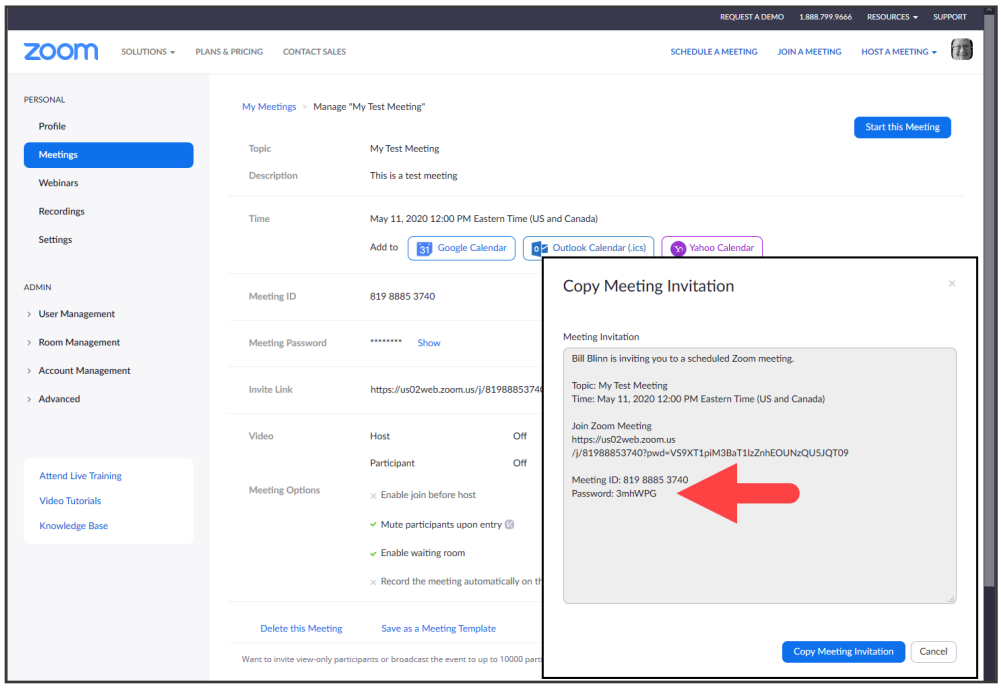
Both (3) host and participant cameras should be turned off initially. This is less a security measure than a way of avoiding the potential for embarrassment if the camera is switched on before the organizer or the participants are ready.

Don't enable (4) the ability for participants to enter the meeting before the host arrives. This is off by default. It's also a good idea to mute participants when they enter the meeting and to enable the waiting room.

With all participants muted, the meeting organizer will need to give someone permission to speak. Leave automatic recording of the meeting off, too. If you need to record a meeting, you can start the recording once the meeting has started.

Once the meeting has been scheduled, Zoom offers the organizer the opportunity to copy a meeting invitation that can then be sent via messenger or email to the participants. If security is a concern, you should avoid using this because it violates a key security practice: The password should never be included in the same message with the login procedure. This suggests that the folks at Zoom still don't quite "get" security.

Zoom's security is getting better and, when meeting organizers are cautious, the service is sufficiently secure for most uses. Ω



When sending the meeting invitation, consider transmitting the password separately instead of including it in the invitation. Using the waiting room creates a bit more work for the meeting organizer, but it's a good safeguard that keeps unwanted meeting crashers at bay.