SpencerFane®

Understanding the Cyber and Privacy Risks Of Zoom and Tips For Using It More Securely

By now everyone has now heard of — and likely used — Zoom for staying connected during the COVID-19 pandemic. In what may have been a brilliant strategy to gain market share during adverse times, Zoom offered its videoconferencing service for free to schools, organizations, businesses, and individuals as a means of staying connected while the world is exercising social distancing and it seems as if everyone is now using Zoom.

With this newfound popularity and attention, however, has come increased scrutiny on the privacy and security issues associated with the Zoom platform. On March 30, 2020, the FBI Boston Division issued a warning about these issues: *FBI Warns of Teleconferencing and Online Classroom Hijacking During COVID-19 Pandemic*

There are countless in depth articles discussing these issues but the two questions people seem to want to know the most are (1) what are the risks of using Zoom, and (2) is there a safer way to use Zoom. Here is the high level version of what's going on with Zoom.

If you do not care about all of the explanation and just want to get to the tips for using Zoom more securely, just scroll down to the end.

For tips on staying more cyber secure in all settings, including working from home, see Spencer Fane's Good Cyber Hygiene Checklist.

Technical Bugs & Vulnerabilities

Zoom has technical bugs and vulnerabilities that are just now being discovered due to the popularity of the service and the massive number of people now testing it for

vulnerabilities – just like any other service. These issues are being fixed as they are identified and likely do not pose that much more of a risk, if any more, than other services of this nature. This is something closely akin to how hackers can use vulnerabilities in applications to turn on your microphone or webcam without you knowing – it is certainly possible, it does happen, but it is rare and, for most of us, because of that rarity, not a primary risk. The best way to help minimize this risk is to make sure that you install any security updates for Zoom applications as soon as they become available as that is how companies like Zoom install "fixes" for these issues.

Phishing / Social Engineering

Because of Zoom's newfound popularity, threat actors are using "Zoom" in all sorts of phishing emails as a means of social engineering to try and get people to click on links to malicious sites, open attachments with malicious code, and be redirected to websites to enter in their private information. The threat actors do this by registering domains that have "zoom" in them, such as a hypothetical www.zoom.freemoney.com or www.freezoomaccount.com or www.zoomallmymoneyoutmybank.com – you get the point. They also do this with online accounts such as Gmail, Yahoo, etc.: Zoom@gmail.com, FreeZoomAccount@yahoo.com, ZoomMeeting@aol.com are not really from Zoom, ok?

It is important to remember that links to Zoom applications, communications, and meeting invites that say "zoom" will only be to a zoom.us or zoom.com URL – anything else using "zoom" in the URL is not authentic and should be ignored.

Privacy Concerns

Zoom is a free service for most, right now. Do you know what that means? The same thing it means for free services like Gmail, Facebook, LinkedIn, Yahoo, and all the rest – if it is free, somehow, YOU ARE THE PRODUCT! This has raised concern about how secure and private the content of information is that you share through Zoom.

Because of these security and privacy issues, there are now government regulators opening investigations into these issues and at least one class-action lawsuit has

been brought against it alleging improper data sharing practices.

As a result of much of the scrutiny it has faced, on March 29, 2020, Zoom updated its Privacy Policy, which you can read here: Zoom Privacy Policy

The terms of Zoom's Privacy Policy permit it to collect and use "data" from when you use Zoom: "We obtain data when you use Zoom in order to deliver our services and provide a better experience to you." This includes several categories but, most importantly:

1. Data that identifies the users.
2. "Customer content," which is described as "information you or others upload, provide, or create while using Zoom," examples of which include "[c]loud recordings, chat / instant messages, files, whiteboards, and other information shared while using the service, voice mails." In other words, this seems to include everything that is communicated via the Zoom platform.

How is this information used?

1. Zoom has stated, "Zoom does not sell customer content to anyone or use it for any advertising purposes." However, other free online services have said similar things in the past. But, just because they do not "sell" the data, does not mean there may not be another way for allowing big data analytics to be run on the data, as a service, and then using the results of such analytics to provide a service to marketing firms, companies, etc. to then use it for advertising purposes – similar to how other free online services have done in the past. I am not saying they do it at all, I do not know firsthand, but, we have seen other "data driven" companies make similar statements.
2. Read the Privacy Policy for yourself and make your own determination, and make sure to consider this language, especially that which I underlined:

   We do not sell your data.

   We do not allow marketing companies, advertisers or similar companies to access personal data in exchange for payment. We do not allow third parties to use any personal data obtained from us for their own purposes, unless you consent (e.g., when you download an app from the Marketplace). Our

customers may use the webinar service to generate their own marketing leads and they may provide marketing information to you. When you register for a webinar, you provide your data to the host of the webinar, and if required, any consent that you give about your data would be to them, as well. Zoom may keep the data about the registration in our system in order to facilitate the webinar, but Zoom does not use or share that data other than to provide the services. A customer may also charge for their webinars. Again, that transaction is between the host and participant of the webinar. Zoom is not selling any data.

As described in the Zoom marketing sites section, Zoom does use certain standard advertising tools on our marketing sites which, provided you have allowed it in your cookie preferences, sends personal data to the tool providers, such as Google. This is not a "sale" of your data in the sense that most of us use the word sale. However, California's CCPA law has a very broad definition of "sale". Under that definition, when Zoom uses the tools to send the personal data to the third-party tool providers, it may be considered a "sale". It is important to know that advertising programs have always worked this way and we have not changed the way we use these tools. It is only with the recent developments in data privacy laws that such activities may fall within the definition of a "sale".

Because of CCPA's broad definition, as is the case with many providers since the CCPA became law, we provide a "Do Not Sell My Personal Information" link at the bottom of our marketing sites. You can use this link to change your Cookie Preferences and opt out of the use of these advertising tools. If you opt out, Personal Data that was used by these tools will no longer be shared with third parties in a way that constitutes a "sale" under CCPA.

3. The bottom line here is, what is being said over the free versions of Zoom may not be truly confidential. This is the same concern I would have for any free service, not just Zoom, and would include other similar videoconferencing platforms. I would be concerned about talking about highly confidential trade secrets (i.e., the secret formula to Coke), HIPAA protected sensitive personal health information, or other things of a particularly sensitive nature over Zoom without first analyzing and addressing how to protect the confidentiality of such

information. The starting point for this analysis should be to look for more secure features of Zoom, such as Zoom for Healthcare which is stated as being HIPAA compliant.

Zoom Bombing – Uninvited Meeting Attendees

Zoom bombing is what you're hearing about the most because it is what people are experiencing the most. This is where someone uninvited just "drops in" on a Zoom meeting and does things such as interrupt, make a fool of themselves, or, share porn one the screen while it is taking place. Here is why it is happening:

1. In its most basic form, Zoom is really just a website location that is hosting the meeting. The host sets it up and the participants get to it via a website URL. Guess what? Anyone else that has that URL can "find" that meeting also and, if the host has not set it up properly, then join the meeting.
2. Personal Meeting ID – Zoom allows users to create a Personal Meeting ID that can be customized by the user. Then, all you have to do is use that Personal Meeting ID to kick-off your meetings and it's always the same – meaning users can always go to the same place / same link for the meeting. This is convenient – it is also scary for when you had someone in a prior meeting and now do not want them in the next meeting you are having.

Note: other videoconferencing services such as WebEx and GoTo Meeting, etc. may have this same capability that can be exploited in the same way.

3. In some cases the problem arises when people are using their Personal Meeting ID to set up multiple meetings and then other people are then "bombing" them with the same ID by joining meetings that they were not invited to.
4. In other cases, Zoom users are sharing their meeting ID's (i.e., the URL) over social media and in other public ways and then many others see that URL and go in and "bomb" the meeting.
5. Finally, just like guessing any other URL, there are people who are simply trying to guess Zoom meeting URLs and finding random meetings and "bombing" them as if it is a game, just to get into mischief as well as for malicious purposes.

Tips for Using Zoom More Securely

So, what are you to do? Does this mean you have to stop using Zoom and find another videoconferencing platform to use?

I do not think so – as I've said several times, any free service you use will have similar concerns and, more importantly, any technological service like this must be used properly to get the most secure and private experience possible.

Many of the problems that are being experienced with Zoom are just like those experienced when using other technology – we always want to enjoy the benefits without accepting the obligations of learning and being responsible for how we use the tool. We have to start by understanding the tool, understanding the inherently public nature of hosting something on the Internet, and learning to use the settings and features that enable you to help make it more secure and private (because absolute security and privacy are impossible on the Internet).

Here are the tips:

- Zoom has a blog with extensive tips on these issues – spend some time on this site: blog.zoom.us
- Make a conscious effort to keep your meetings private – especially those with children. There are two options for doing this: require a meeting password or use the waiting room feature and control the admittance of guests.
- Disable "Join Before Host" unless otherwise needed, that way the host can keep control over attendees.
- Do not use your Personal Meeting ID for public events and, understand, anyone who you share that Personal Meeting ID with will continue to have it long after your meeting with them is over. Plan accordingly.
- The meeting host should maintain control over who is joining the meeting and set it so that if someone is removed, they cannot come back into the meeting. Do this by disabling "Allow Removed Participants to Rejoin" feature.
- Make it so only the Host can screenshare, unless otherwise needed.
- Disable the "File Transfer" feature unless otherwise needed.
- Do not post meeting URLs on social media or in other public forums unless you want it open to everyone on the Internet – and I can't see many reasons to do

that!

This blog post was drafted by Shawn Tuma, a Partner in the Plano, TX office of Spencer Fane LLP. For more information, visit www.spencerfane.com.