Legal Tech: Zoom Conferencing Security

By Trey Peacock, Winning Cases Based On Science & Data For Over 25 Years
Originally published on LinkedIn.com

As the world transitions to a place in which we try to remain separate from one another, we are all feeling the impact of social distancing and self-isolation. Technology has surged forward to fill the resulting gaps in our social and professional lives. As a result, the use of Zoom, a web-conferencing app, has skyrocketed. Offices, schools, and social gatherers alike are using Zoom to easily and quickly host group meetings by video chat. Zoom's popularity likely results from several factors: its simple user interface offers faster and easier workflow than comparable apps like Skype or Google Hangouts; its licenses are affordable; and its functionality works quite well in both professional and casual settings.

In the wake of Zoom's new-found popularity, however, potential users in both the private and public sector have voiced concerns about the integrity of Zoom's software security. Some companies, like Elon Musk's Tesla, have prohibited their employees from using the software at all. Much of the criticism about Zoom stems from its meeting creation and entry mechanism: most meetings require admission via invitation or entry code. While Zoom never publicizes or lists these meeting IDs, a hacker or troll could theoretically gain access to a meeting either by

guessing random combinations of numbers and letters or by discovering a given meeting's code. Many of the reported breaches of Zoom have occurred in college and school settings that used widely distributed meeting links. While these unauthorized entrances are somewhat rare, they still present a concern for those using Zoom for matters that require more security than a quarantine happy hour.

Zoom, for its part, has responded quickly and robustly to the security concerns. CEO Eric Yuan has admitted that, in the face of the COVID-19 crisis the company moved a bit too fast with its platform and failed to address some privacy issues. The company has vowed to do better going forward. On April 5th, Yuan said the company will pause all feature-based improvements for 90 days in order to focus on constructing and pushing out security-focused updates.

To be sure, Zoom's default software setup is lacking in certain areas. However, for most users, it should not be eschewed. With the few tweaks and techniques listed below, most professionals and social users can protect their meetings, devices, and accounts from unauthorized access.

Update Your Software

As Zoom races to address the vulnerabilities in its software, it has pushed and will continue to push new software updates which patch holes and beef-up security protocols. By consistently checking for new updates and installing them promptly, users can ensure they run the most secure version of the Zoom software. Accordingly, in the coming weeks and months, installing updates remains one of the quickest and easiest ways to increase or maintain security.

Change Meeting Settings

While some choose to download Zoom's proprietary application onto their computer or mobile device, others will choose to simply use Zoom's web interface to join and host meetings. Whichever path you take, be sure to alter your default settings as outlined below to better protect the integrity of your meetings. Logging into your Zoom account on your web browser provides the easiest method for changing the default settings on your account. Once changed, these settings should apply to your user account across all platforms.

First, ensure that you generate a new, unique meeting ID for each Zoom session you host. This ID should obviously not be distributed to anyone other than the intended meeting participants and should be discarded at the meeting's close.

Second, always require that, in addition to the meeting ID, users enter a password to gain entrance to the session. Again, this password ought to be unique and used only once. Users have the option to send a unique, encrypted hyperlink to their meeting attendees, which will automatically enter the password and meeting ID when followed. Users should, as always, take care to ensure that the link is distributed securely.

Third, change the screen-share options so that only the host can control whose screen is visible. This maintains a measure of control over sensitive information in case an unauthorized party enters the meeting. With this feature turned on, the host will be able to quickly turn off any active screen, protecting potentially confidential documents or images.

Finally, turn on the option allowing the host to always show the meeting control bar. In a moment of crisis, the few precious seconds spent searching for the Hold or Mute buttons could allow an intruder time to view or access sensitive content. In addition, having this bar handy allows the Host to better manage and supervise the participants in the meeting.

Do Not Use Your Personal Meeting Room

Zoom offers users the ability to host a meeting from their personal user room. However, this option is considerably less secure than creating a new meeting room. Zoom gives each user room a number ID, but that number stays consistent across every meeting, and can potentially be hacked. Always use the "New Meeting" option from the Zoom menu and identify the meeting with a unique meeting ID and password combination.

Carefully Manage Meeting IDs

Either when distributing the unique ID/password combo or the meeting hyperlink, ensure that your attendees receive the meeting entry information through a secure medium, such as a private company email server. Additionally, carefully review the list of recipients to ensure no unintended parties, such as support staff or past clients, receive the meeting info. Ensure all attendees understand that the meeting ID should not be forwarded or distributed to anyone. This step further limits the possibility that a meeting ID will be discovered through a phishing scam or other system breach. In addition, prohibit the sharing of a meeting ID on any form of social media including Twitter, Facebook, or LinkedIn. If an attendee is approached by a party asking for the meeting ID for any reason, the request should be referred to the host for review.

Be Vigilant as a Host

If you find yourself hosting meetings for your company or group, understand that you bear the primary responsibility for ensuring your meeting's security. Following the steps listed above when creating and distributing your meeting ID will help protect the integrity of the invitation. However, as a host, you should also carefully monitor the attendees during the meeting. While this can be difficult with large groups, those are exactly the type of meetings that require vigilance to prevent an unauthorized user from masquerading as an attendee. Accordingly, require each attendee to use a label with a unique user ID that you possess and can verify. A unique user ID can be as simple as a name or title, but requiring these labels prevents large numbers of attendees with screen names like "ZoomUser" or a simple phone number and allows the host to more easily identify intruders or uninvited attendees. Additionally, when possible, ask attendees to keep their camera on at the outset of a meeting to allow for visual verification of each attendee's identity.

If you discover an unrecognized or unauthorized user at any point, immediately pause the meeting and disable any active screen-sharing. Request that the user unmute and identify themselves orally or visually. If the user's identity cannot be confirmed, disconnect the user from the meeting. To be clear, once you disconnect a user, there is no way to let them back into the meeting.

These tips, employed together, should significantly decrease the security risks posed by the current gaps in Zoom's software. Users should stay apprised of future developments in the software, either in the form of new vulnerabilities, or updates for patching previous faults.

About the Author

Trey Peacock, a partner at Susman Godfrey, has been winning cases based on science and data for over 25 years. He has also chaired the firm's IT committee for over two decades. Learn more about Trey here.