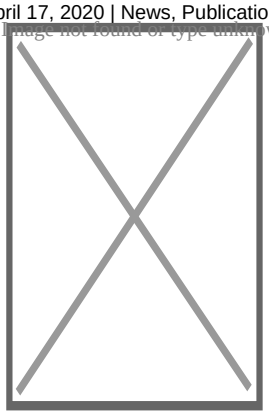
NINE BEST PRACTICES TO PROTECT YOUR NEXT VIRTUAL-TELECONFERENCING MEETING

April 17, 2020 | News, Publications



Co-Authored by: **Mitch Merchant** and **Mark Zukowski**

With more than 65% of us working from home, clients and legal professionals are relying on virtual-teleconferencing (VTC) platforms, such as Zoom, GoToMeeting and WebEx. Zoom provides users a super-simple user experience, which has no doubt contributed to its 20x jump in usage over the past few months. Unfortunately, it's this ease of use that made Zoom vulnerable to attacks and thus were thrust into the spotlight in both the best and the worst way.

"Zoombombing" is discussed daily in mainstream and social media outlets, making us hyper sensitive to the security issues of our VTC platforms. Not surprisingly, there is a lot of hyperbole in the media right now, because hyperbole generates clicks and clicks generate revenue. The growing pains faced by Zoom and other VTC platforms are quite public, and even minor security issues take on major importance.

The good news for the 65% of us WFH is that most VTC platforms, especially Zoom, have been quick to act and very transparent about their ongoing issues. Users are provided regular updates regarding security patches and policies. Furthermore, Zoom recently announced a 90-day pause on other initiatives to devote its engineering resources exclusively to privacy and security.

Here are nine best practices to implement today to avoid becoming a target of a Zoombombing during your next VTC meeting:

1. Always protect your online meetings with a randomly generated password. Do not create your own meeting password. The meeting host can take this security precaution one step farther and create unique invite links specific to each authorized participant.
2. Never use the same Meeting ID twice. Zoom will automatically generate a new Meeting ID for each meeting you schedule. However, there is also an option to create a Personal Meeting ID (PMI) specific to you, the host. This is not encouraged, but if you MUST use your own PMI, create a new ID each time. This will prevent those who know your PMI (possibly from attending a meeting you hosted previously) to jump into a meeting that's active and one in which they may not have been invited.
3. Always connect using your full name and email address. This will ensure the meeting host can quickly identify all participants and kick-out anyone who isn't invited.
4. Never connect to a VTC meeting using public WiFi. It's best to use a hard-wired ethernet connection with a strong password. If you must use WiFi, use your own from home or office, and ensure your network name and password is not easily guessed.
5. Always check your surroundings to avoid inadvertent eavesdroppers. This shouldn't be a problem if you're connected from your home office or regular work office, but it's important that each participant takes control over their environment.
6. Never share the meeting link or password with parties who are NOT invited to your meeting. Many of the recent cases of Zoombombings were not actually hacked, but rather, the meeting host posted the link on a public social media channel, essentially inviting ne'er-do-wells to join. Further, these meetings were often hosted by new users – such as educators – and not seasoned Zoom users who already used advanced security measures.
7. Always update the software when prompted and ensure you're using the latest version. VTC platform providers are regularly updating their software to provide additional and enhanced security.
8. Never allow participants to control the screen sharing feature. Only the host should have control over which participants can share their screen and when.

9. Always communicate a technology failure protocol with participants, in the event your meeting is hacked. This can be as simple as instructing participants to immediately leave the meeting, then call the host's phone number instead.

Each day, there are more security patches and additional best practices to protect your meetings. Right now, VTC platforms such as Zoom are low hanging fruit. That doesn't mean your meeting should be.

For further information on the FBI's warning regarding online meetings, visit fbi.gov.

click here to download the pdf

Mitch Merchant is JSH's Director of IT, ensuring secure, prompt and innovative technology service and accessibility. Mitch is responsible for developing and managing the firm's security plan, including off-site storage and cloud-based storage, as well as software development, network engineering, database design, and providing firm employees immediate technical support through the JSH Help Desk. Prior to joining JSH, Mitch worked for five years at Intel Corp as an engineer and 15 years with regional law firms as a network administrator and engineer. He earned his B.S.E. in Electrical Engineering from Arizona State University.

Mark Zukowski is a partner and online mediator at JSH. He has conducted more than 600 mediations and arbitrations throughout his 20+ years of providing ADR services. With social distancing affecting case progression, he now provides virtual face-to-face mediation services for all civil and tort claims. Parties can rely on the same professional resource without the risk of in-person meetings. Mark has been a litigator for more than 39 years and has tried 25 cases to verdict. He received extensive training through the American Arbitration Association (AAA) and the Straus Institute for Dispute Resolution at Pepperdine University. He is a diplomate member of the prestigious National Academy of Distinguished Neutrals (NADN).