PY &T Powell Youngblood & Taylor LLP

ED CLIPS!

Unwanted Guests – The FBI Warns of Zoom Bombing

Jill Williams

As more Americans rely on the virtual world for work, online classes, and to keep connected with loved ones amid the COVID-19 pandemic, the Federal Bureau of Investigation is warning of potential hijacks of videoconferencing applications.

The popular videoconferencing app Zoom has seen a massive increase in users since the pandemic has forced many people to stay at home. Consequently, Zoom-bombing, the practice of unwanted guests intruding on video meetings for malicious purposes, has also significantly increased. These internet trolls take advantage of open and unprotected meetings and poor default settings to take-over screen sharing and broadcast porn or other explicit material.

In late March 2020, the FBI warned the public of the potential for Zoom-bombing, after two schools in Massachusetts saw their online classes get hijacked on Zoom. A teacher in Massachusetts reported that while she was conducting an online class using Zoom, an unidentified individual(s) dialed into the classroom. The individual shouted profanity and then shouted the teacher’s home address in the middle of the instruction. The same week, a second Massachusetts school reported a Zoom meeting being accessed by an unidentified individual whose image was visible on the video screen displaying swastika tattoos.

YouTube has become a platform for hackers to brag about successful Zoom-bombing “pranks.” These YouTubers post videos of themselves interrupting videoconferences for their YouTube channel subscribers. These videos typically show the participants who were on the screen at the time of the “prank,’ and their reaction to the intruders as they shout profanities and other explicit remarks.

The FBI warns that in addition to those who take over screen sharing as a “prank, there have been more serious reports of cybercriminals creating domains that impersonate Zoom to steal personal information.

Zoom-bombing can happen to anyone, but it makes sense to try to reduce your risk as much as possible. As individuals, schools, and other businesses continue to transition to online lessons and meetings, it is imperative that users exercise due diligence and caution in using any videoconferencing sites or applications. Zoom wrote a recent blog, “*How to Keep Uninvited Guests Out of Your Zoom Event*,” that includes tips on how to avoid getting caught by this issue along with a list of some great added features to help secure your Zoom event and host with confidence. Below are some helpful tips for those hosting meetings on Zoom.

- Password protections are on by default, and it recommends that users keep those protections on to prevent uninvited users from joining a meeting.
- Hosts are encouraged to review their settings and confirm that only the host can share their screen. Do not make meetings and classrooms public.
- Be sure all user’s software is updated
- Provide a link directly to those invited to the meeting or classroom. Avoid sharing a Zoom meeting link in a public forum, as anyone who has the link can join the meeting.
- Use the Waiting Room feature where a host can only allow people in from a preassigned register. The Waiting Room is a virtual staging area that stops your guests from joining until you are ready for them. Meeting hosts can customize Waiting Room settings for additional control and can personalize the message people see when they hit Waiting Room, so they know they are in the right spot.
- Lock the meeting. When you lock a Zoom meeting that has already started, no new participants can join.
- For extra security, users should set up a password entry system. This is effectively a two-factor authentication for participants to use before entering the chat. This password should only be shared privately.
- Remove unwanted or disruptive participants. You can mouse over a participant’s name, and several options will appear, including Remove.
- Disable video. Hosts can turn someone’s video off, which will allow hosts to block unwanted, distracting, or inappropriate gestures on video.
- Mute participants. Hosts can mute/unmute individual participants or all of them at once.
- Disable private chat. Zoom has an in-meeting chat for everyone, or participants can message each other privately. Restrict participants’ ability to chat amongst one another while your event is going on to cut back on distractions.
- Report all incidents to Zoom on their website so they can take appropriate action.

Zoom responsibly, and please join Powell, Youngblood & Taylor, LLP, and the Texas Rural Education Association for the next **“COVID-19 Rural Roundtable”** where TREA panelists discuss updates such as Zoom-bombing and share innovative rural district solutions to COVID-19 continuity of services. We will send out details for this upcoming webinar soon, but for now, please visit our website, www.pyt-law.com, to access our latest COVID-19 resources, including Client Alerts, The School Zone Podcasts, and our recent webinars.