How to Avoid ‘Zoom Bombing’ and Other Tele Video-Conferencing Tips

As the novel Coronavirus continues to impact our daily lives, the use of remote conferencing systems to conduct meetings are becoming ubiquitous and unfortunately, are more vulnerable to hackers. The term 'zoom bombing' describes when a hacker gains access to a Zoom meeting with the goal of disrupting the video chat by inserting inappropriate and/or offensive materials in their video feed (pornographic materials, hate speech, etc.) The Federal Bureau of Investigation (FBI) describes this as video-teleconferencing (VTC) hijacking and has received multiple reports of conferences being disrupted by the FBI Boston Division. While the FBI provides important measures to prevent hackers from disrupting online meetings, such as setting meetings to private, cities and villages must comply with public notice requirements and as such, are uniquely vulnerable to disruption. Here are some tips to ensure your VTC meetings are safe and secure.

**Restrict video sharing, turn off file transfer options, doodle options, and mute all participants.**
Typically, the host of a meeting has the ability to change screen-sharing settings. Check your products screen-sharing settings and, if possible, select “host only” in the screen-sharing settings. Zoom and other services allow you to turn off settings such as “file transfer” options and “annotation” which prevents a guest from sharing any files or doodling and marking up content with everyone. Within settings, you can also mute participants that are in the meeting as well as new participants joining a meeting which is particularly useful not only for preventing disruption from a hacker, but also to reduce ambient noise and feedback such as barking dogs.

**Don’t use your Zoom personal ID meeting.**
Services such as Zoom have a personal meeting ID associated with each user profile. Because that ID does not change, sharing it publicly increases the risk that future meetings using that same personal ID could be Zoom bombed. Use the ‘schedule meeting’ capability of Zoom which will generate a one-time meeting ID. If you have already utilized your account’s personal ID for a previous meeting, contact Zoom directly to request to have your personal ID changed.

**Enable a waiting room.**
Products such as Zoom have ‘waiting rooms’ which is a feature that allows the host to control when a participant joins the meeting. Participants can be admitted into the meeting one by one, or you can hold all attendees in the waiting room and admit all at once when you are ready. Additionally, you can customize the waiting room screen with your own logo or information. This is useful if you want to set ground rules for the meeting and protocols for banning anyone who violates the rules of the meeting.

**Remove participants from the meeting.**
If a participant is disrupting a meeting, you can remove them from the meeting. Make sure to turn off “allow removed participants to rejoin”. This option will ensure someone who has been removed cannot rejoin and cause further disruption. Some services also allow you to put a meeting ‘on hold’ which will disable video and audio momentarily in the case of a disruption.