FLASTER GREENBERG
Attorneys at Law | A Professional Corporation

Tips On Protecting Your Virtual Meetings To Avoid A Cyber Security Breach

Blog Post

April 9, 2020

Krishna Jani & Donna Urban

Virtual Meetings, and their Unintended Vulnerabilities

Advanced technology and the availability of online video and teleconferencing software has certainly helped ease the transition to working remotely for many businesses, schools, health care providers, and even the Courts. However, these virtual meeting platforms, while increasingly popular and essential especially during the COVID-19 pandemic, are not always completely secure.

Over the past few days, you may have seen the term Zoom-Bombing circulating around the news. This term refers to nefarious actors, or trolls, on the web hijacking Zoom and other virtual meetings to display a variety of disruptive, and often disturbing, behavior. This computer hacking creates serious privacy concerns as it exposes confidential and sensitive material, such as medical information, financial data, trade secrets, and other proprietary information, to these intruders and other third parties.

Protect Your Meetings from Uninvited Guests

We suggest taking the following steps to help keep your virtual meetings closed to intruders:

- **Create a random or randomly-generated meeting number for each meeting.** Zoom, and other virtual meeting platforms such as GoToMeeting or Skype for Business, allow for a standing meeting number but reports have indicated that such standing meeting numbers are being sold on the dark web. In at least one instance, stolen account information such as email addresses, passwords, meeting identifications, type of account, host keys, and names were actively being sold or posted to the dark web. In other instances, sensitive information from virtual meetings was discoverable through a search engine on the open web. Even a United States healthcare provider, seven educational institutions, and one small business were targeted in such virtual meeting cyberattacks.
- **Ensure that each meeting is password-protected.** For example, Zoom can automatically create a password and does with each new meeting. In the alternative, when creating the invitation, the meeting creator can assign a password in the invitation. The password will then be included in the meeting invitation that is sent out to the attendees.
- **Lock virtual meetings once theyre in session.** Some virtual platforms allow for meeting creators to lock their meetings once theyre in session. To prevent unexpected attendees from joining a current session, lock your meeting or enable a virtual waiting room. Youll be notified when an attendee attempts to join and can easily connect all waiting attendees to the meeting by unlocking.

These precautions should help keep your virtual meetings free from any unwanted Zoom-Bombers.

Further Guidance

To further address these emerging privacy concerns, on April 8th, Senator Edward Markey, whose priorities include telecommunications, technology, and privacy policy, urged the Federal Trade Commission to publish industry cybersecurity guidelines for online conference providers for protecting consumers privacy.

If you have any questions, please feel free to reach out to Donna Urban, Krishna Jani, or any member of Flaster Greenbergs Telecommunications or Privacy & Data Security Groups.

Donna T. Urban is a member of Flaster Greenbergs Commercial Litigation and Environmental Law Departments concentrating her practice in telecommunications law, environmental regulation and litigation, and privacy and data security. She is a seasoned litigator, and for more than 20 years has successfully represented business clients in contract disputes, regulatory matters, and complex negotiations. She can be reached at donna.urban@flastergreenberg.com or 856.661.2285.

Krishna A. Jani is a member of Flaster Greenbergs Litigation Department focusing her practice on complex commercial litigation. She is also a member of the firms cybersecurity and data privacy law practice groups. She can be reached at 215.279.9907 or krishna.jani@flastergreenberg.com.