Privacy and Cybersecurity Tips for Zoom Meetings

Over the last few weeks, Zoom has quickly become the way we stay connected – with colleagues, with friends, with family. Whether you're using Zoom for internal meetings, client engagement, virtual happy hours, or coffee breaks, you want to be sure that privacy and confidentiality are top of mind.

The New York Times reported that the New York Attorney General is looking into Zoom's privacy practices, based in large part on another report stating that the Zoom app sent data to Facebook without informing its users. The data Zoom sent was high level data about usage – **no sensitive or confidential company information –** and **Zoom has already addressed the issue and is no longer sending ANY user data to Facebook.**

This news gives us an opportunity to look more closely at the options in Zoom that we can use to protect our privacy, and to protect the confidentiality of the meetings we're having on the platform. We always strive to balance usability and flexibility with security and while we have implemented certain Zoom security features broadly to protect meetings, additional capabilities are available to you as meeting organizers should you decide that an extra level of security is appropriate.

Manage attendees and ensure no unwanted guests

- **Try the Waiting Room**: Consider using the Waiting Room feature. It is a virtual staging area that stops attendees from joining until you're ready for them.
  - Click on the Settings (gear) icon in the Zoom app, and click on View Advanced Features to launch the Zoom web portal configuration. Under In Meeting (Advanced) turn on the Waiting Room.
- **Lock the meeting**: You can lock a Zoom Meeting that's already started, and no new participants can join, even if they have the meeting ID and password (if there is one).
  - In a meeting, click Manage Participants at the bottom of your Zoom window. In the Participants pop-up, click More and choose Lock Meeting from the dropdown.

Avoid using your Personal Meeting ID (PMI) for sensitive conversations

- Your PMI is basically one continuous meeting. If you want to prevent people who you've met with before from joining a confidential meeting, you can generate a random meeting ID.
  - Use the Schedule button from the Zoom app, and under Advanced options, make sure the Use Personal Meeting ID button is *not* checked
  - You can also password protect a meeting with a random meeting ID for additional security.

Manage Screen Sharing

- "Zoombombing" has become a common occurrence, where a potentially uninvited or unwelcome meeting attendee shares his/her screen with offensive content. In order to eliminate this risk, meeting organizers should maintain control of the screen at all times
- To prevent participants from screen sharing during a call, using the host controls at the bottom, click the arrow next to Share Screen and then Advanced Sharing Options. Under "Who can share?" choose "Only Host" and close the window.

We are here to help. If you have any questions about how to maintain good cybersecurity hygiene while working remotely, please don't hesitate to contact Please e-mail security@blackstone.com

Blackstone