BlueJeans Publishes Eight Best Practices for Safe Videoconferencing During COVID-19

Submitted by: Round Earth Consulting
Thursday, 2 April 2020

Guidelines designed to help workers across industries stay safe as videoconferencing usage soars 3x in just over a month

BlueJeans Network (http://www.bluejeans.com), which provides videoconferencing services in more than 180 countries, today released “8 Best Practices for Safe Videoconferencing During COVID-19.” These guidelines are designed to ensure the safety and security of organisations and their people, many of whom are adapting at breakneck speed to remote meetings, events and service delivery.

Recent usage data (https://www.bluejeans.com/blog/video-conferencing-usage-during-coronavirus-outbreak) released by BlueJeans shows how fast employees around the globe have shifted from working in offices to working from home since the beginning of the COVID-19 outbreak. In less than two months, countries across nearly every continent saw a 100 to 300 percent increase or more in video conferencing traffic, compared with baselines pre-COVID-19 breakout.

In large Western European countries for example as of 27 March 2020, daily average conferencing traffic for BlueJeans Meetings had grown by 194% in France, 278% in Italy, 289% in the UK, 350% in Germany and 509% in Spain, compared to the average daily usage prior to COVID-19 breakout dates in late February.

In the rush to move meetings and events online to support employees working from home, BlueJeans recommends people follow eight guidelines to avoid the most common types of videoconferencing security and privacy breaches:

1. Be careful about sharing your Meeting ID - Though you may want to recruit as many people as possible to your meeting or live event, exposing your Meeting ID on social media, websites or other public forums can attract the wrong kinds of attendees. There are many examples where attendees have shared unsavoury content in ‘all-welcome’ events. Be extra vigilant about this if your meeting involves children. As a minimum precaution we recommend using a One-Time Meeting ID. By not revealing your Personal Meeting ID to the public, your future meetings won’t attract unwanted guests.

2. Always use passcodes - Meeting hosts should apply both moderator and participant passcodes (if available) to heighten meeting security. Moderator Passcodes require the meeting host (or a designated delegate) to enter a unique code to start the meeting. This prevents risky behaviour happening before the host arrives. Participant Passcodes add an additional layer of security, allowing only those with the correct code to join the meeting. Some videoconferencing services offer advanced fraud detection to detect and report on repeated login failures and meeting join failures. This helps block the type of malicious intruders who scan for meeting IDs over a set period of time.

3. Know your provider’s data privacy policy - while it can be tedious to read the fine print on data privacy, you don’t want to sleepwalk into a situation that compromises your business and its employees. While most providers share some level of data with third parties, the devil is in the details. Some provide personal data on individual participants to third parties; others only provide aggregated data on

call information such as duration, location and number of participants. If a system shares personal data with third parties, most countries' laws require you to communicate this to meeting participants. Ask your legal counsel for advice on any policy wording that's not clear.

4. Keep watch on meeting joiners - Meeting hosts have the ability to track who joins meetings in a variety of different ways, depending on the system they're using. Most allow the host to set an audible alert to announce when new attendees join. Some also display entry and exit banners with the names of joining attendees on-screen. The host should also view the meeting roster to verify who is on the videoconference. If unrecognised or anonymous names are on the list, the host should ask them to confirm their identity by voice or chat.

5. Master the controls - To prevent unwanted participants joining your meeting or event, make sure the system you're using allows the host to eject or drop a participant and prevent them from re-joining. Some systems also let you lock a meeting once all of the required individuals are present, critical when participants plan to cover sensitive and confidential information. A common problem occurs when a meeting host with back-to-back meetings uses their Personal Meeting ID. One meeting overruns and the participants for the next call join, listening in to the previous meeting. If you expect this to happen, plan in advance and use a One-Time Meeting ID.

Most systems allow hosts to mute the audio and video of some or all participants, and put the meeting in 'host-only' mode. This helps keep the group focused and prevents disruptions, including from unwanted guests. Participants that want to ask questions have other options, depending on the system. Some allow people to virtually 'raise their hands' then ask questions by voice or chat.

Beware that some platforms enable file transfers which can be conduits for malware sharing. At the least, ensure that meeting hosts can disable 'file transfer' to prevent malware being shared.

6. Use live meeting controls for large meetings and events - When companies need to run large meetings or events with more than 25 people, they should invest in systems with appropriate capabilities and security features. Systems designed for larger groups allow hosts to delegate the job of monitoring and controlling the meeting participants, and also moderate question and answer sessions.

7. Use browser-based meetings to avoid download delays - Some platforms require people to install software, delaying meeting start times. If you want to avoid participants having to download software before joining, look for videoconferencing providers that support browser-based options that use the WebRTC real-time communications standard, where users can simply click on a link to join a meeting in a web browser.

8. Practice basic security hygiene - According to online security experts Check Point, 90% of cyberattacks start with a phishing campaign. If you receive a link by email or social channels to join a videoconference, contact the sender to confirm its legitimacy. Never open links and attachments in emails from unknown senders. Look for the classic clues of cybercrime like spelling errors in URLs and emails.

"Our data shows the incredible effort taking place at great speed by organisations and people around the world to help stem the spread of COVID-19 by working from home," commented Alagu Periyannan, CTO

and Co-Founder, BlueJeans Network. “We hope these guidelines will help people stay safe and healthy at home, while maintaining secure business operations and protecting personal information during this incredibly challenging period.”

Resources
+ For information about worldwide BlueJeans usage trends watch this video (https://bluejeans-1.wistia.com/medias/hm60o3xsk6).
+ For information about video conferencing growth in Europe, watch this video (https://bluejeans-1.wistia.com/medias/rpdvpgsfj1).
+ For more information about BlueJeans security features please visit this page (https://www.bluejeans.com/products/secure-video-conferencing) or review our Technical Security and Privacy Guide here (https://www.bluejeans.com/sites/default/files/security-and-privacy.pdf).
+ Check this blog post (https://www.bluejeans.com/blog/secure-video-conferencing-protecting-your-home-office-meetings) for a quick refresher regarding BlueJeans’ security features.

About BlueJeans Network
BlueJeans is the meetings platform for the modern workplace and the first cloud service to connect desktops, mobile devices and room systems in one video meeting. Thousands of organisations across industries use BlueJeans every day for video, audio and web conferencing meetings and large interactive events, so people can work productively where and how they want. For more information, visit www.bluejeans.com.

Press Contact:
Sarah Lafferty
Round Earth Consulting
+44 7917 222 144
slafferty@roundearthconsulting.com
Twitter @ladylaff