CRENSHAW, WARE & MARTIN, PLC

VIDEO CONFERENCING BEST PRACTICES

Cybersecurity Data Incident Hotline

(757) 802-9043
cybersecurity@cwm-law.com

Darius K. Davenport

ddavenport@cwm-law.com

150 W. Main Street, Suite 1500, Norfolk, VA 23510
P: (757) 623-3000 | F: (757) 623-5735 | www.cwm-law.com

Video Conferencing Security Best Practices

With many employees transitioning from the office to teleworking from home, video conferencing has surged in popularity and demand. Wherever your work takes you, consider these best practices to increase the security of your next video conference:

1. **Secure Connection**

   With a quick online search, you can stay abreast of the latest vulnerabilities associated with most web conferencing platforms. Following basic tips from security experts will protect your online meetings from compromise.

2. **Avoid Unwanted Visitors and Content**

   To ensure the content of your video conferencing is shared only with its intended participants:

   - Do not post meeting links (i.e. Zoom, WebEx, MS Teams) on public websites or social media.
   - Do not use your personal meeting ID for meetings.
   - Do not allow participants to share their screen, or require the host to approve participant desktop sharing.
   - Disable file transfers unless you know the files to be shared and file sharer.
   - Enable features that prevent removed participants from rejoining a meeting.
   - Add a passcode to your meetings and only share that passcode with your attendees.
   - Enable features that allow participants to join and interact before the host enters.
   - Restrict meetings to only authenticated users if feasible.
   - Enable "waiting room" features prior to starting meetings so that you can identify participants before letting everyone in.

3. **Take Advantage of Built-In Security Bells and Whistles**

   Scheduling and configuring the details of your upcoming video conference is best done within the conferencing platform so you can take advantage of the built-in security features.

   - If available, ensure encryption is turned on, within the software, for each video conference.
   - Use a web camera cover so no one else can use your camera without your knowledge.
   - Do not record the video conference unless truly necessary.
   - Use background blur, digital backgrounds, or greenscreen settings to conceal information about your location.
   - Turn off any "attention tracking" features that track participants during a screenshare.
   - Enable muted microphones as default setting.

4. **Your Privacy Matters**

   Get rid of the crumbs left behind that leave evidence of your video conferencing call so you can avoid unwanted marketing and hackers.

   - Use a unique email address specifically for video conferencing.
   - Clear cookies and block trackers after every video call.
   - Opt out of all secondary data uses where possible.
   - When there is a privacy issue, leave feedback with the service about the problem.
   - Use other devices for communications during video conferences.

150 W. Main Street, Suite 1500, Norfolk, VA 23510
P: (757) 623-3000 | F: (757) 623-5735 | www.cwm-law.com