Using Video Conferencing Services Safely

The world has been moving into a more digital and online environment. This is very evident for those that work from a remote location. Remote workers have realized the importance of using video conferencing services such as Zoom, Microsoft Teams, Cisco Webex, etc. These conferencing options are key for employees and employers to communicate, collaborate and meet when working remotely.

It's important to ensure you are mindful of security when utilizing any video conferencing software. The following best practices are recommended when using a video conferencing service.

1. Only download these applications/services from the provider itself to avoid accidentally installing malware on your computer. Ensure you have the most up-to-date software.

2. Don't use the same ID for all of your meetings. Set up a unique meeting ID for every scheduled conference. Otherwise, it makes it easier for hackers to video-bomb your meetings or record them.

3. Set up a waiting room area for your video conferences. This way you can see everyone that wants to join the meeting and screen them before letting them into the conference. This is a good way to prevent video-bombers from causing a disruption to your meeting.

4. Provide a meeting link directly to those you wish to invite to the meeting. Do not send a broadcast email with the meeting link.

5. Provide a password for your video conference to help prevent unwanted attendees from crashing your meeting.

6. Make sure there is only one host for your meeting and this person is the only one that can control screen-sharing, video and mute options, record options and allow guests into the meeting.