Videoconferencing at Service Coordination Support, including Developmental Services Ontario Eastern Region

Security Risks and Best Practices

April 2020

Table of Contents

Introduction 3
Video Conferencing Security Risks 3
Video Conferencing Security Tips 4
Creating and Hosting Meeting Responsibility (Moderator) 5
Best Practices for Effective Video Conferencing 6
Tips to improve a video conferencing meeting: 7

Video Conferencing at SCS (including DSOER)

Introduction

Due to the recent situation regarding COVID-19 and the directed measures of physical (social) distancing, our employees have been directed to continue meeting with clients/families via either telephone or videoconferencing, if possible.

SCS, including DSOER, uses the BlueJeans conferencing software, which is a secure platform to conduct virtual meetings (videoconferences) with clients. Please note that there will always be security risks with any online communication platforms – See Security Risk and Best practices below in this document. Employees initiating a videoconference meeting via BlueJeans will be responsible for hosting the meeting.

Employees at SCS, including DSOER, are permitted to participate in a videoconference on another platform of your choice (i.e. Zoom), but employees will ensure that you are aware of the security risks and will be asking you a few questions before they proceed in participating in a videoconferencing software/platform of your choice.

By asking you these few questions, SCS (including DSOER) will not be held responsible for any privacy breach/issue that occurs. You will be responsible for hosting the videoconference on the platform of your choice.

The questions you will be asked when initiating a videoconference on the software/platform of your choice are the following:

- Are you aware of the security risks associated with the use of videoconferencing platforms/software?
- Is this platform/software secured with a unique ID# and password?
- Does this platform/software have the ability to track the participants' identity when they are entering the videoconference?
- To your knowledge, is this platform/software upgraded to the latest updated version?

Staff may refuse to participate on the platform of your choice if they have concerns about the security of the information, depending on your responses to the questions above.

Video Conferencing Security Risks

With the rise in popularity of video conferencing for business meetings, remote education and virtual social gatherings due to the current situation, miscreants have started a series of new attacks targeting video conferencing technologies and their users.

Here are examples of some of the attacks:

- **Meeting Bombing** – In this type of attack, an uninvited guest joins a video conferencing meeting either to listen in on the conversation or to disrupt the meeting by sharing inappropriate media. Prevent unwanted access by using unique ids and passwords for each meeting
- **Malicious Links in Chat** – Once attackers gain access to your meeting room, they can trick participants into clicking on malicious links shared via the chat, allowing attackers to steal credentials. This reinforces that it's more critical than ever to require passwords for all meetings.
- **Stolen Meeting Links** – Reusing meeting links makes it easy for attackers to use them too. To avoid unauthorized access to your meetings, turn on notifications that will let you know when someone has joined your meeting room without you. Or better yet, don't allow others to join your meeting before you do by disabling "Join Before Host."
- **Data Shared With Third Parties** – Ensure security controls are in place to protect your data, and then ensure those controls are configured properly. Be aware of the participants of the meeting and the files you are sharing that have confidential or personal information. It important to have data protection agreements in place with third parties that address appropriate security controls.
- **Malware or Zero Day Attacks** – When it comes to zero day attacks, legacy anti-virus software is no match. You will need to protect from malicious activity by layering security at the endpoint and in the network.

Video Conferencing Security Tips

- Never re-use a meeting ID
- Password protect all meetings
- Enforce identification of participants either by showing video or verbal acceptance
- Never share any links or meeting ID's on social media
- File sharing should be only be shared with appropriate participants (permissions to share)

- Screen sharing should be done with appropriate participants to protect personal information
- Report any suspicious activity to your administrator

Creating and Hosting Meeting Responsibility (Moderator)

1. **Require Passwords:** As a meeting host, this is the No. 1 action that you can take to secure your meetings: Make passwords mandatory for all your meetings to protect against uninvited guests and to secure information about the meeting, including meeting name and organizer.
2. **Verify Attendees:** Be sure to check the attendee list when sending out the meeting invitation, and review the participants list during the call. Remove anyone on the call who is not supposed to be a part of the meeting.
3. **Check Meeting Links:** When you receive a meeting invitation, verify that it's from a known, trusted sender. Also, check the meeting link before clicking, watching out for malicious links with ".exe," for example. There's a steep rise in phishing attempts where malicious links have the names of video conferencing vendors embedded but they take you to phony login sites. By using password-embedded links, you will increase security and reduce war dialing, a technique used to discover or guess the meeting ID.
4. **Patching**: Make sure your video conferencing software is patched with the latest vendor-provided updates and have automated upgrades turned on.
5. **Keep Confidentiality:** Keep confidential conversations private, and be sure you're not accidentally sharing anything confidential on your laptop or in your background. Virtual backgrounds have gained popularity for a change of scenery!
6. **Review Your Security Settings:** Review and enable appropriate security and privacy settings to prevent threat actors from exploiting known vulnerabilities.
7. **Report Suspicious Activity:** Remember to report any suspicious activity to your corporate Information Security and Information Technology teams.

Best Practices for Effective Video Conferencing

To make your video conferencing meetings more productive and rewarding for everyone, review the general video conferencing best practices and learn how to improve the experience whether you are an onsite participant or a remote participant.

Follow these tips to ensure a more successful video conferencing meeting.

Prior to a meeting:

- When using equipment or locations not regularly used, test your meeting connections in advance.
- When possible, establish online video conferencing connections several minutes before the meeting start time.
- Create a backup communication plan in case you have trouble connecting with remote participants. A backup plan can include asking onsite participants to connect to the meeting through their laptops, using a mobile or speakerphone, and/or collaborating through an online collaboration tool.

During a meeting:

- Have all participants share their video and audio. No “lurkers”.
- Ensure all participants can see and hear all other participants, as appropriate.
- Ensure conference room microphones are distributed appropriately to pick up all speakers.
- Ensure location lighting does not limit a participant’s visibility (e.g., avoid backlighting from windows or lamps).
- Have participants mute their microphones if their location has excessive background noise or they will not be speaking.
- Have a meeting facilitator. Often, but not always, the person who called the meeting. The facilitator is responsible for:

  - providing an agenda to participants. Ahead of the meeting is nice, but minimally at the start of the meeting, which includes an overview of topics to be covered and planned outcome;
  - establishing the visual or verbal cues, such as raising a hand, to indicate when someone wants to actively contribute verbally to the meeting;
  - engaging participants at all locations to ensure discussion understanding, and alignment;
  - limiting “side conversations” and multitasking or ensure all participants are made aware of that content;
- Make sure all participants have equal access to content by sharing all content within the video conferencing connection and using online tools

Tips to improve a video conferencing meeting:

If you participate remotely in a video conference, follow these instructions to ensure the best experience.

- Ensure the strength of your internet connection. If weak, you can try to connect via a wired Ethernet jack. This prevents Wi-Fi dropouts and speed issues.
- If connecting from a laptop, plug in the laptop wall power. Battery use can adversely affect video quality.
- Test the connection before the call; this is strongly recommended.
- Ensure that you have a camera, microphone, and headphones or speakers available. Earbuds or headphones are preferable to avoid audio feedback and echo. Most modern laptops and all-in-one desktops have a headphone jack, microphone, and speakers built in.
- Be aware of your surroundings and how you appear visually.
  - Call from a quiet location with no background noise.
  - Close blinds on windows so that you are easier to see on video.
  - Wear neutral, solid-colored clothing. Avoid black, white, or striped clothing.
- Be aware of your behavior. Because you are on a video conference, people can see what you are doing at all times, including read your lips.

- Be aware that IT cannot troubleshoot while you are on a video conference so test in advance and schedule help long before your meeting.
- Follow all instructions in the video conferencing invitation and note important supplemental information, such as a backup phone number in case you are disconnected.