Best Practices for Conducting Virtual Meetings

July 2020

With the increasing popularity of videoconferencing technology, the number of bad actors seeking to exploit vulnerabilities in the software continues to grow. While no videoconferencing software can guarantee 100 percent protection from threats and MOAA is not recommending a particular software solution, the following are recommended best practices for users when planning and executing a virtual meeting.

1. Make sure you and your participants are using the latest version of the virtual meeting software and all updates are current.

2. Make sure you and your participants are using the Windows 10 operating system or a newer operating system and all of the updates are current.

3. Use the waiting room feature in videoconferencing software. This feature allows the host to only admit people who are authorized to join the meeting. If participants join via the call-in option, ensure they are positively identified before the meeting begins.

4. Make sure password protection is enabled and if the software allows you to create a password for the meeting, use password creation best practices, such as a random string of numbers and symbols – not "password" or "123456."

5. Don't share links to virtual meetings via social media posts. Invite attendees from within the conferencing software and ask your attendees not to share the links. Also, send the videoconference link close to the event start time to minimize the possibility of sharing.

6. Don't allow participants to share their screen by default. The host should manage screen sharing.

7. Encourage all participants to mute their microphones when not in use and use the "chat" or "hand-raising" function to signal their interest in speaking.

8. Lock the meeting once all participants have joined the videoconference.

9. Don't record meetings unless required and make sure you announce the meeting is being recorded. If you elect to record a meeting, give it a unique name – not the default name – when you save it.

10. Check to make sure software security settings are on by default.

Virtual meetings are an excellent resource to keep your volunteer leaders informed and engaged. Following these best practices will help to keep your meeting secure and protect the data of all meeting participants.

###