Best Practices for Virtual Meetings

Meeting Organizers / Hosts

The following are best practices meeting hosts should follow to help ensure a successful meeting:

- Provide the following when sending out meeting invitations:
  - Remind participants that Zoom, MS Teams and Webex meetings may be accessed without downloading the application. Although some of the features may not be available, each tool offers the ability to join meetings via a web browser;
  - Notification that the meeting is going to be recorded;
  - Collaboration tool guidance documents and/or links; and
  - The best practices for participants, listed below.

- Do not publish meeting password/passcodes - If the meeting requires a password, the password should not be made public, and it should be sent directly to the invited participants. In the event the meeting participants are unknown, and the meeting URL must be made public, participants should be encouraged to contact the meeting organizer for the password. Please note - If the password is embedded in the URL, meeting attendees will not be prompted to enter the password and will be able to access the meeting without requesting the password.

- Familiarize yourself with the meeting platform's security features - For the foreseeable future, the majority of meetings will remain virtual, and therefore the threat of malicious actors attempting to access and disrupt meetings will also remain. To minimize the potential of "Zoom bombings" and other malevolent tactics, meeting hosts must be aware of the meeting platform's security features and how to access them; be vigilant during the course of meeting to watch for malicious activity; and be comfortable deploying the security feature if the need arises.

- Be able to recognize the signs of malicious use of a collaboration tool aka "Zoom bombing" – Such as a malicious actor:
  - Screen sharing inappropriate images (violent, pornographic, racist, sexist, etc.) and/or anything not a part of the meeting's topic;
  - Disrupting the meeting conversation with inappropriate sounds and/or words;
  - Uploading files that contain viruses and/or inappropriate material; and/or
  - Accessing, leaving, and re-entering meetings with the same or different accounts.

- Enable your web camera - Web cameras enhance the level of communication that can be achieved during virtual meetings. Turning on your camera will encourage meeting participants to do the same. There are several other benefits to consider:
  - Increases security - malicious actors are easy to visually identify and remove;
  - Facial expressions and body language are visible - Communication becomes far more efficient and engaging when facial expressions and body language are in play;
  - Reduces the feeling of isolation - Web cameras allow attendees to see each other, simulating the feeling of being co-located and reducing the feeling of isolation that occurs after weeks of teleworking; and
  - Ensures continual meeting engagement by attendees - Being on camera reduces the likelihood of attendees multi-tasking during meetings.

- State whether the meeting is being recorded. This will inform participant unfamiliar with or unable to see the tool's visual recording queue.

- Share a specific application or browser instead of an entire desktop - To prevent accidentally exposing sensitive information, while enhancing the visual experience of participants, opt to share specific applications and/or browser windows.

Participants

The following are best practices that meeting participants should follow to help ensure a successful meeting:

- Access the meeting 2-3 minutes prior to when it is scheduled to begin. This will allow the time needed to overcome potential issues connecting to the meeting.
- Select either phone or computer audio – When joining the meeting only select one audio option, either the phone line or computer audio, but not both.
- Mute yourself – Mute your line whenever you are not speaking. If your line is not muted, background noise will interfere with the meeting audio.
- Identify yourself – When speaking during the call, especially if you have not spoken in several minutes, identify yourself by name. This will help the host and meeting participants to follow the call and recognize your voice.
- Speak directly into the handset/headset/microphone – To ensure meeting participants can hear you clearly, speak directly into your microphone.
- Enable your web camera - Facial expressions and body language will be visible. Communication becomes far more efficient and engaging when facial expressions and body language are in play.
- Refrain from side conversations – During a conference call, only one person should speak at a time. Side bar conversations prevent attendees from hearing and following the primary conversation.
- Confidentiality – Meetings may be recorded, so use caution when sharing information that could be captured.