Teleconferencing Security Tips

With the transition to work from home there is an increase of cyber attacks against the technologies we use to communicate. One recent example of this is what has been coined “ZOOM BOMBING”. Malicious individuals joining teleconferences uninvited and posting explicit video and audio.

The State’s standard for teleconferencing is **WebEx** and this bulletin is not promoting Zoom. We are aware that some vendors that you interact with leverage this technology. Also, for parents your children’s school may be using these technologies as well. Feel free to share these tips with whomever you wish.

We recommend exercising due diligence and caution in your cybersecurity efforts. The following steps can be taken to mitigate teleconference hijacking threats if you host meetings:

WebEx Best Practices:

Auto Lock Personal Room for secure meetings. This prevents all attendees in your lobby from automatically joining in the meeting. The host will see a notification when attendees are waiting in the lobby and as the host, you will authorize the attendees to join. This can be done from My Webex > Preferences > My Personal Room on your Webex site.

Set Personal Room Notifications before a Meeting to receive an email notification when attendees are waiting for a meeting to begin. You will then be able to review the participant list and expel any unauthorized attendees.

Schedule a Meeting instead of using your Personal Room. Personal Rooms web links do not change. Improve security by scheduling a meeting which includes a one-time web link.

Scheduled Meetings are unlisted by default by the Site Administrator for all Webex sites. Unlisting Meetings enhances security by requiring the host to inform the meeting attendees, either by sending a link in an email invitation, or hosts can enter the meeting number using the Join Meetings page. Listing a meeting reveals meeting titles and meeting information publicly.

Set a password for every Meeting by creating a high-complexity, non-trivial password (strong password). A strong password should include a mix of uppercase and lowercase letters, numbers and special characters (for example, $Ta0qedOx!). Passwords protect against unauthorized attendance since only users with access to the password will be able to join the meeting.

Do not reuse passwords for meetings. Scheduling meetings with the same passwords weakens meeting protection considerably.

Use Entry or Exit Tone or Announce Name Feature to prevent someone from joining the audio portion of your meeting without your knowledge. This feature is enabled by default for Webex Meetings. For notifications, select Audio Conference Settings > Entry and exit tone > Beep or Announce Name. Otherwise, select No Tone.

Do not allow attendees or panelists to join before host. This setting is set by default by the Site Administrator for Meetings.

Assign an alternate host to start and control the meeting. This keeps meeting more secure by eliminating the possibility that the host role will be assigned to an unexpected, or unauthorized, attendee, in case you inadvertently lose your connection to the meeting. One or more alternate hosts can be chosen when scheduling a meeting. An alternate host can start the meeting and act as the host. The alternate host must have a user account on your Webex Meetings website.

Lock the meeting once all attendees have joined the meeting. This will prevent additional attendees from joining. Hosts can lock/unlock the meeting at any time while the session is in progress.

Expel Attendees at any time during a meeting. Select the name of the attendee whom you want to remove, then select Participant > Expel.

Teleconferencing Security Tips

Share an Application instead of sharing your Screen to prevent accidental exposure of sensitive information on your screen. Ex. Microsoft Office products, Web browsers, etc.

Set password for your recordings before sharing them to keep the recording secure. Password-protected recordings require recipients to have the password in order to view them.

Delete recordings after they are no longer relevant.

Create a Host Audio PIN. Your PIN is the last level of protection for prevention of unauthorized access to your personal conferencing account. Should a person gain unauthorized access to the host access code for a Personal Conference Meeting (PCN Meeting), the conference cannot be started without the Audio PIN. Protect your Audio PIN and do not share it.

Do not click on emails where you don't know the sender, email has inconsistencies with grammar and/or spelling, or contain a web link you're unfamiliar with.

Zoom Best Practices:

Do not make meetings or classrooms public. In Zoom, there are two options to make a meeting private: require a meeting password or use the waiting room feature and control the admittance of guests.

Do not share a link to a teleconference or classroom on an unrestricted publicly available social media post. Provide the link directly to specific people.

Add a passcode to your meeting, then share that passcode with your guests. Once set, the passcode is required in order to enter the meeting.

Manage screensharing options. In Zoom, change screensharing to “Host Only.”

Ensure users are using the **updated version** of remote access/meeting applications.

Do not use Facebook to sign in: It might save time, but it is a poor security practice and dramatically increases the amount of personal data Zoom has access to.

Use two devices during Zoom calls: If you are attending a Zoom call on your computer, use your phone to check your email or chat with other call attendees.

Don't use your personal meeting ID for meetings. A Zoom Personal meeting ID is the same as a Personal Room meeting in WebEx.

Consider turning on the “waiting room” for your meeting so that you can scan who wants to join before letting everyone in.

If you don't want participants to join/interact before the host enters, **uncheck "Join Before Host**". Set an alternate host if you need a backup host.

Disable "Allow Removed Participants to Rejoin" so that participants who you have removed from your session cannot re-enter.

Disable "File Transfer" unless you know this feature will be required.

Disable annotation if you don't need it.