Video Teleconference Security Tips – April 2, 2020
California Department of Technology, Office of Information Security

FBI released an article; warning users of teleconferencing sessions being hijacked (also being referred to as “Zoom-bombing”) all over the nation. The FBI has received multiple reports of conferences being disrupted by pornographic and/or hate images and threatening language. In the wake of reports of this activity being reported to the FBI’s Internet Crime Complaints Center (IC3 -ic3.gov), they have published the following recommendations:

- 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.
- Manage screensharing options. In Zoom, change screensharing to “Host Only.”
- Ensure users are using the updated version of remote access/meeting applications. In January 2020, Zoom updated their software. In their security update, the teleconference software provider added passwords by default for meetings and disabled the ability to randomly scan for meetings to join.
- Lastly, ensure that your organization’s telework policy or guide addresses requirements for physical and information security.

Additionally, the Department of Homeland Security (DHS) Cybersecurity and Infrastructure Security Agency (CISA) released a notice today about regarding this activity and added the following recommendations as this issue is not specific to Zoom, but rather applies to all video teleconferencing (VTC) software:

- Consider security requirements when selecting vendors. For example, if end-to-end encryption is necessary, does the vendor offer it?
- Ensure VTC software is up to date.

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.

Many State entities are standardizing on Microsoft Teams for teleconferencing and we are not promoting Microsoft Teams nor WebEx/Zoom in this bulletin. 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 your workforce in your entity.

Office of Information Security (OIS) recommends exercising due diligence and caution in your cybersecurity efforts. The following steps can be taken to mitigate teleconference hijacking threats if you host meetings.

Specific User Security Best Practices for Video Teleconferencing tools:

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. In WebEx 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 Weber 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 strong password where required 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.

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

Assign an alternate host when possible 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.

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 a participant and remove/expel an attendee.

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 (when recordings are required) 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.

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.

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

Ensure users are using the **updated version** of any remote access/meeting applications they use. Regularly check and apply software updates.

Do not use Facebook or any other social media site to sign in: It might save time, but it is a poor security practice and dramatically increases the amount of personal data meeting tools have access to.

For increased security use two devices during web conferencing calls: If you are attending a video teleconferencing 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.

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.

In Microsoft Teams: Remove guests from **persistent meeting spaces** (when not needed): Meeting hosts can remove the guest from the persistent meeting space. When inviting a guest, meeting organizers need to be aware of what a guest has access to during, and after the meeting. For more details on MS Teams guests refer to: https://docs.microsoft.com/en-us/microsoftteams/guest-experience#comparison-of-team-member-and-guest-capabilities