Judicial Council Information Technology

Technology Advisory and Best Practices for Video Teleconferencing

April 21, 2020

Background

With the transition to work from home there is an increased use of video technologies to communicate, leading to an increase in related cyber-attacks. One example is "Zoom Bombing," in which malicious individuals join a video teleconference (VTC) uninvited and post explicit video and audio (such as sharing pornographic and/or hate images and threatening language). Federal agencies such as the Federal Bureau of Investigation (FBI), the Department of Homeland Security (DHS), and the Cybersecurity and Infrastructure Security Agency (CISA) have issued warnings and recommendations to address these concerns.

FBI Warning and Recommendations

Recently, the FBI warned of video teleconference sessions being hijacked (or "Zoom-bombed") nationwide. As a precaution, the FBI's Internet Crime Complaints Center (IC3) published the following recommendations:

1. **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.
2. **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.
3. **Manage screensharing options.** In Zoom, change screensharing to "Host Only."
4. **Ensure users utilize 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.
5. **Ensure that your organization's telework policy or guide addresses requirements** for physical and information security.

Other Federal Warnings and Recommendations

DHS and CISA recently released a notice regarding this activity and added the following recommendations as this issue is not specific to Zoom, but applies to all VTC software:

1. **Consider security requirements when selecting vendors.** For example, if end-to-end encryption is necessary, does the vendor offer it?

2. **Ensure VTC software is up to date**.

Best Practices for Video Teleconferencing Use

The following best practices identify specific features and settings within various applications – such as Zoom and WebEx – but comparable features may exist and be applied to multiple platforms.

Meeting Setup and Invitations

1. **Schedule a Meeting instead of using your Personal Room**. Personal Room web links do not change. Improve security by scheduling a meeting which includes a one-time web link. *In WebEx, scheduled meetings are unlisted by default by the Site Administrator. Unlisted meetings enhances security by requiring the host to inform the meeting attendees of the event, either by sending a link in an email invitation or entering the meeting number using the Join Meetings page. Listing a meeting reveals meeting titles and meeting information publicly.*
2. **Do not use your Personal Meeting ID** to host meetings. *A Zoom Personal Meeting ID is the same as a Personal Room Meeting in Webex.*
3. **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 to control guest admittance.*
4. **Auto-Lock Personal Room for secure meetings**. This prevents all attendees in your lobby from automatically joining the meeting. The host will see a notification when attendees are waiting in the lobby and, as host, will need to authorize the attendees to join. *In Webex this can be done from My Webex > Preferences > My Personal Room on your Webex site.*
5. **Set a strong password where required** for every meeting that is complex and non-trivial (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.
6. **Do not reuse passwords** for meetings. Scheduling meetings with the same passwords weakens meeting protection considerably.
7. **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.
8. **Do not share a link to a video teleconference or classroom on an unrestricted publicly available social media post**. Provide the link directly to specific attendees.
9. **Do not click on emails** in which you do not know the sender, that contain text with grammatical and/or spelling errors or inconsistencies, or that contain an unfamiliar web link.
10. **Disable "File Transfer**" unless you know this feature will be required.
11. **Disable annotation** if you do not need it.

Meeting Sign-in and Management

1. **Do not use Facebook or any other social media site to sign in**. This method might save time, but it is a poor security practice and dramatically increases the amount of personal data accessible to meeting tools.
2. **Assign an alternate host when possible** to start and control the meeting. This keeps the 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.
3. **Do not allow attendees or panelists to join before host**. This setting is typically set by default by the Site Administrator for meetings.
4. **Consider turning on the "waiting room**" feature for your meeting so that you can scan who wants to join before letting everyone into the conference.
5. **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.
6. **Disable "Allow Removed Participants to Rejoin**" so that participants who you have removed from your session cannot re-enter.
7. **Lock the meeting** once all attendees have joined the meeting. A lock will prevent additional attendees from joining. Hosts can lock/unlock the meeting at any time while the session is in progress.
8. **Use Entry and Exit Tones** or Announce Name Features to prevent someone from joining the audio portion of your meeting without your knowledge.
9. **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.
10. **Share an application instead of sharing your screen** to prevent accidental exposure of sensitive information on your screen. Examples of applications include Microsoft Office products, Web browsers, etc.
11. **Manage screensharing options**. *In Zoom, for example, change screensharing to "Host Only."*
12. **For increased security, use separate devices while multi-tasking during web conferencing calls**. If you are attending a video teleconference on your computer, use your phone to check your email or chat with other call attendees.

Post-Meeting

1. **Set a 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.
2. **Delete recordings** after they are no longer relevant, making sure to follow applicable records retention requirements.