Do’s and don’ts of Videoconferencing Services

As part of its advisory, many offered safety tips for companies, schools and individuals using videoconferencing services. After speaking with other security experts, we’ve expanded on those ideas to create this list of web meeting security do’s and don’ts.

- ✓ Do use waiting room features in conferencing software. Such features put participants in a separate virtual room before the meeting and allow the host to admit only people who are supposed to be in the room.

- ✓ Do make sure password protection is enabled. Make sure that your service uses both a meeting ID number and a string, but in addition, that it also has a separate password or PIN. If the service lets you create a password for the meeting, use password creation best practices — use a random string of numbers, letters, and symbols; don’t create an easily guessable password like“123456.”

- ✓ Don’t share links to teleconferences or classrooms via social media posts. Invite attendees from within the conferencing software — and tell them to not share the links.

- ✓ Don’t allow participants to screen share by default. Your software should offer settings that allow hosts to manage the screen sharing.

- ✓ Don’t use video on a call if you don’t need to. Turning off your webcam and listening in via audio prevents possible social engineering efforts to learn more about you through background objects.

- ✓ Do use the latest version of the software. Security vulnerabilities are likely to be exploited more often on older software versions.

- ✓ Do eject participants from meetings if an intruder is able to get in or becomes unruly. This prevents them from re-joining.

- ✓ Do lock a meeting once all the participants have joined the call. However, if a valid participant drops out, be sure to unlock the meeting to let them back in and then re-lock it after they return.

- ✓ Don’t record meetings unless you need to. If you do record a meeting, make sure all participants know they are being recorded (the software should indicate this)

- ✓ Do educate all employees who host meetings on the specific steps they should take in the software your company uses to ensure their conferences are secure.

A list of recommended security settings for people who use Video Conferencing App for personal meetings. Here's a summary of his recommendations:

- ✓ Turn off [Participants Video]. They can turn it back on once you allow them to join.
- ✓ Turn off [Join before host]
- ✓ Turn off [Use Personal Meeting ID (PMI) when scheduling a meeting]
- ✓ Turn off [Use Personal Meeting ID (PMI) when starting an instant meeting]
- ✓ Turn on [Require a password when scheduling new meetings]
- ✓ Turn on [Mute participants upon entry]
- ✓ Turn on [Play sound when participants join or leave] (this is heard by host only).
- ✓ Turn on [Screen Sharing] - host only
- ✓ Turn off [Annotation]
- ✓ Turn on [Breakout room] - allows host to assign participants to breakout room scheduling.
- ✓ In the advanced settings, hosts should Turn on [Waiting Room] feature.