PRAIRIE VIEW A&M UNIVERSITY

A Member of the Texas A&M University System

April 2, 2020

TO: Faculty and Staff

FROM: Henry Rose
Security Analyst II

RE: FBI Warns of Teleconferencing and Online Classroom Hijacking During COVID-19 Pandemic

As large numbers of people turn to video-teleconferencing (VTC) platforms to stay connected in the wake of the COVID-19 crisis, reports of VTC hijacking (also called "Zoom-bombing") are emerging nationwide. The FBI has received multiple reports of conferences being disrupted by pornographic and/or hate images and threatening language.

Within the FBI Boston Division's area of responsibility (AOR), which includes Maine, Massachusetts, New Hampshire, and Rhode Island, two schools in Massachusetts reported the following incidents:

- In late March 2020, a Massachusetts-based high school reported that while a teacher was conducting an online class using the teleconferencing software Zoom, an unidentified individual(s) dialed into the classroom. This individual yelled a profanity and then shouted the teacher's home address in the middle of instruction.
- A second Massachusetts-based school reported a Zoom meeting being accessed by an unidentified individual. In this incident, the individual was visible on the video camera and displayed swastika tattoos.

As individuals continue the transition to online lessons and meetings, the FBI recommends exercising due diligence and caution in your cybersecurity efforts. The following steps can be taken to mitigate teleconference hijacking threats:

- Do not post Zoom/WebEx links on other sites, only in eCourses or through PVAMU official email
- When creating a meeting, always require a password
- Do not allow the meeting to start unless the host arrives - create a meeting room
- Meetings should be private, not public
- Perform a virtual role call if possible
- Lock the meeting once everyone is in
- Enable host-only sharing. If other users are allowed to share their screens to present to everyone else, grant the users permission to share only when required.
- Be cautious of what is in chat
- If audio is breaking up, dial by phone and use the video to view the presentation
- Be careful of fake emails or popups instructing you to install Zoom. Zoom should only be installed by going to https://pvpanther.zoom.us/.
- If you receive a request to support you, please be sure that this is a prearranged meeting with your support personnel. The request should come from a PVAMU user and an official PVAMU account.

For step-by-step guidance on how to secure your Zoom meetings, please visit: Tips for securing your Zoom meetings.

For more tools, tips and application support, visit: www.pvamu.edu/telecommuting.