FLORIDA DEPARTMENT OF EDUCATION
fldoe.org

MEMORANDUM

TO: School District Superintendents

FROM: Jacob Oliva

DATE: April 2, 2020

SUBJECT: Cyber Security Best Practices & FBI Warning Following Several Reports of Video, Teleconference Hacks

As Florida school districts have transitioned to distance learning and online education, please be aware that cyber security hackers are indeed poised to capitalize during a crisis. Below are things you can do to protect yourself and your school district or college:

- Make sure devices are up to date on anti-virus protection.
- Use multi-factor authentication on any accounts for which it is available.
- Only work on secure, password-protected internet connections.
- Avoid accessing any confidential or sensitive information from a public WiFi network.
- Be aware of phishing emails designed to entice you to click on the latest and greatest offer related to coronavirus protections, or with urgent instructions from your boss or co-worker. The intent is to get you to unsuspectingly download malware onto your device and the district or college system.
- Avoid using Bluetooth in a public place – it is an easy way for hackers to connect to your device.
- Be sure to report any lost or stolen device immediately to minimize the risk of fraud.

The Florida Department of Education has also developed a webpage for distance learning that includes a helpful video outlining cybersecurity tips. Feel free to utilize these resources and share them with your information specialists, teachers and students.

In addition, the Florida Fusion Center at the Florida Department of Law Enforcement issued the following alert for situational awareness:

Florida Fusion Center
Situational Awareness

Please see the NOC Media Monitoring Report below regarding the Federal Bureau of Investigation (FBI) issuing a warning about the potential for video-conferencing call hijackings. These video-teleconferencing hijackings are known as “Zoom-bombing” and can potentially disrupt conferences or classes with pornographic, hate, or threatening images. The FBI advises making meetings and classrooms private and require users to enter a password to participate.

Location(s): United States

- As businesses and schools turn to online and digital solutions during social distancing intended to combat the coronavirus outbreak, the Federal Bureau of Investigation has issued a warning about the potential for video-conferencing call hijackings, according to media Monday.
    - Reports of video-teleconferencing hijacking (VTC), also known as "Zoom-bombing," have emerged across the world and multiple reports have been filed with the FBI of conferences and classes being disrupted with pornographic and/or hate images and threatening language.
    - The FBI Boston Division reported two schools in Massachusetts fell victim to "Zoom-bombing" in March.
        - One local high school reported that, while a teacher had been conducting an online class through Zoom, an unidentified person dialed into the classroom, yelled a profanity and then shouted the teacher's address in the middle of the lesson.
        - A second Massachusetts school reported someone infiltrated in one of their Zoom meetings.
            - In this incident, the person was visible through their computer's camera and displayed images of swastikas.
        - Additionally, on Sunday, a sermon live streamed by the First Baptist Church in Jamaica Plain was hacked by a Colorado man who began spouting off homophobic rants and gibberish.
    - As people continue to use VTC for business and teaching purposes, the FBI recommends being careful and cautious in cyber security efforts, primarily making meetings and classrooms private and requiring participants to enter a password to participate.

JO/he