Public Service Announcement

FEDERAL BUREAU OF INVESTIGATION

December 15, 2020

Alert Number I-121520-PSA

Questions regarding this PSA should be directed to your local **FBI Field Office.**

Local Field Office Locations: www.fbi.gov/contact-us/field-offices

Transition to Distance Learning Creates Opportunities for Cyber Actors to Disrupt Instruction and Steal Data

This PSA was written with contributions from the Cybersecurity and Infrastructure Security Agency (CISA).

The FBI is raising awareness for parents and caregivers of school-age children about potential disruptions to schools and compromises of private information, as cyber actors exploit remote learning vulnerabilities.

Video Conference Disruptions

When used for real-time instruction, unsecured video conferences are vulnerable to disruption by unauthorized users (e.g., students not enrolled in the class, parents/guardians, or strangers). According to complaints received by the FBI, interruptions include verbal harassment of participants and teachers, use of offensive language, and displaying images containing pornography and violence.

Social Engineering and Phishing

Cyber actors rely on social engineering tactics, such as phishing, to deceive victims into revealing personal information or performing a task. Cyber actors can take advantage of the increased reliance on electronic communications between students, parents, and teachers to craft fraudulent emails. For example, a cyber actor can use the compromised email of a school official to request private information, send a victim to a malicious website, or convince a victim to download a malicious attachment. This could lead to the compromise of home computers or identity theft.

Cyber actors also register web domains that are similar to legitimate websites to capture individuals who mistype URLs, such as ending a school's name with *.com* rather than *.edu*. Subtle changes in website URLs could easily go unnoticed by a user, such as adding or changing a single character. For example, a user wanting to access *www.cottoncandyschool.edu* could mistakenly click on *www.cottencandyschool.edu* (changed one “o” to “e”) or *www.cottoncandyschoo1.edu* (changed letter “l” to a number “1”).[a] Victims who believe they have clicked on a legitimate link are in reality visiting a site controlled by a cyber actor.

Recommendations

The FBI recommends parents and caregivers implement cybersecurity best practices to minimize the effect of cyber attacks. At minimum, parents and caregivers of students engaged in distance learning should confirm local/home computer networks are secure by implementing basic cybersecurity measures at home and monitor device use to minimize risks to online safety.

Cybersecurity Best Practices at Home:

- Ensure personally owned devices run the latest version of the operating system
  - Upgrade devices running Windows 7 to Windows 10
- Ensure firewalls are properly configured and secure on routers and computers
- Replace default router passwords with strong, unique administrative passwords or passphrases
- Enable multi-factor authentication for all applications when this option is available
- Install software and application updates as soon as they are released
- Update and/or confirm wireless routers and other hardware are operating the most recent firmware
- Ensure personally owned computers use up-to-date antivirus, antispyware, etc.
- Teach children to recognize and report suspicious email messages and html links to an adult

Distance Learning Best Practices:

- Identify a point of contact at your school for questions relating to the security of school-issued devices
- Identify a point of contact at your school to report cyber incidents involving distance learning
- Understand how software and firmware updates are implemented on school-issued devices (e.g., automatic updates versus updates requiring user action)
- Change default passwords for school applications when permissible by the school
- Monitor children’s online activities for unusual contacts or accessing suspicious web sites that are not affiliated with distance learning content

[a] This is a fictitious example to demonstrate how a user can mistakenly click and access a website without noticing subtle changes in website URLs.

- Consider covering device cameras when not in use for class sessions
- Confirm online conferencing platforms used by students are requiring passwords or other authentication methods (such as validation from hosts)
    - Emphasize to students not to share meeting passwords or html links

General Child Data Exposure Best Practices:

- Monitor privacy settings and information available on social media sites
- Conduct regular Internet searches of children's information to help identify potential exposure and spread of their information online
- Consider credit or identity theft monitoring to check for fraudulent use of child identities
- If possible, provide minimal amounts of information on children when creating online accounts and user profiles (e.g., use initials instead of full names, avoid using exact dates of birth, do not include photos)

Additional Resources

- FBI's Safety Online Surfing Program - A free educational program for children that teaches cyber safety and helps them become better digital citizens in a fun and engaging way: https://www.fbi.gov/about/community-outreach/safe-online-surfing-sos-program
- FBI Boston Press Release (March 2020) reporting a number of video teleconferencing incidents and mitigation strategies for users: https://www.fbi.gov/contact-us/field-offices/boston/news/press-releases/fbi-warns-of-teleconferencing-and-online-classroom-hijacking-during-covid-19-pandemic.
- CISA Tip: Avoiding Social Engineering and Phishing Attacks
- CISA and CYBER.ORG "Cyber Safety Video Series" for K-12 students and educators
- CISA Cybersecurity Recommendations and Tips for Schools Using Video Conferencing

Victim Reporting

The FBI encourages victims to report suspicious or criminal activity to their local FBI field office, and to file a complaint with the Internet Crime Complaint Center (IC3) at www.ic3.gov. In addition, report incidents involving distance learning or education technology tools to your child's school.