Public Service Announcement

FEDERAL BUREAU OF INVESTIGATION

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.

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:

- Replace default router passwords with strong, unique administrative passwords or passphrases
- 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:

- For questions relating to the security of school issued devices please contact,
- (Mr. Minieri, michael.minieri@totowa.k12.nj.us or Mr. Cheng, alvin.cheng@totowa.k12.nj.us)
- To report cyber incidents involving distance learning please contact, Mr. Bower for WPS (david.bower@totowa.k12.nj.us) or Mr. Compel for MS (joseph.compel@totowa.k12.nj.us)
- Understand how to update windows machines on school-issued devices
- **Monitor children's online activities for unusual contacts or accessing suspicious web sites that are not affiliated with distance learning content**
- Consider covering device cameras when not in use for class sessions
- 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
- 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
- CISA Tip: Avoiding Social Engineering and Phishing Attacks
- CISA and CYBER.ORG "Cyber Safety Video Series" for K-12 students and educators

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.