Public Service Announcement
FEDERAL BUREAU OF INVESTIGATION

Sep 13, 2018

Alert Number
I-091318-PSA

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

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

Education Technologies: Data Collection and Unsecured Systems Could Pose Risks to Students

The FBI is encouraging public awareness of cyber threat concerns related to K-12 students. The US school systems' rapid growth of education technologies (EdTech) and widespread collection of student data could have privacy and safety implications if compromised or exploited.

EdTech can provide services for adaptive, personalized learning experiences, and unique opportunities for student collaboration. Additionally, administrative platforms for tracking academics, disciplinary issues, student information systems, and classroom management programs, are commonly served through EdTech services.

As a result, types of data that are collected can include, but are not limited to:

- personally identifiable information (PII);
- biometric data;
- academic progress;
- behavioral, disciplinary, and medical information;
- Web browsing history;
- students' geolocation;
- IP addresses used by students; and
- classroom activities.

Malicious use of this sensitive data could result in social engineering, bullying, tracking, identity theft, or other means for targeting children. Therefore, the FBI is providing awareness to schools and parents of the important role cybersecurity plays in the securing of student information and devices.

Sensitive Student Data

The widespread collection of sensitive information by EdTech could present unique exploitation opportunities for criminals. For example, in late 2017, cyber actors exploited school information technology (IT) systems by hacking into multiple school district servers across the United States. They accessed student contact information, education plans, homework assignments, medical records, and counselor reports, and then used that information to contact, extort, and threaten students with physical violence and release of their personal information. The actors sent text messages to parents and local law enforcement, publicized students' private information, posted student PII on social media, and stated how the release of such information could help child predators identify new targets. In response to the incidents, the Department of Education released a Cyber Advisory alert in October 2017 stating cyber criminals were targeting school districts with weak data security or well-known vulnerabilities to access sensitive data from student records to shame, bully, and threaten children.

Cybersecurity issues were discovered in 2017 for two large EdTech companies, resulting in public access to millions of students' data. According to security researchers, one company exposed internal data by storing it on a public-facing server. The other company suffered a breach and student data was posted for sale on the Dark Web.

Inter-connected Networks and Devices

EdTech connected to networked devices or directly to the Internet could increase opportunities for cyber actors to access devices collecting data and monitoring children within educational or home environments. Improperly secured take-home devices (e.g. tablets, laptops) or monitoring devices (e.g. in-school surveillance cameras or microphones), particularly those with remote-access capabilities, could be exploitable through cyber intrusions or other unauthorized means and present vulnerabilities for students.

Recommendations

The increased use of connected digital tools in the learning environment and widespread data collection introduces cybersecurity risks of which parents should be aware.

The FBI recognizes there are districts across the United States who are working hard to address cybersecurity matters in their schools to protect students and their data. For districts seeking assistance, there are numerous online resources, consortiums, and organizations available that can provide support on data protection matters and cybersecurity best practices.

The FBI encourages parents and families to:

- Research existing student and child privacy protections of the Family Educational Rights and Privacy Act (FERPA), the Protection of Pupil Rights Amendment (PPRA), the Children's Online Privacy Protection Act (COPPA), and state laws as they apply to EdTech services.
- Discuss with their local districts about what and how EdTech technologies and programs are used in their schools.
- Conduct research on parent coalition and information-sharing organizations which are available online for those looking for support and additional resources.
- Research school-related cyber breaches which can further inform families of student data vulnerabilities.
- Consider credit or identity theft monitoring to check for any fraudulent use of their children's identity.
- Conduct regular Internet searches of children's information to help identify the exposure and spread of their information on the Internet.

If you have evidence your child's data may have been compromised, or if you have experienced any of the Internet crimes described in this PSA, please file a complaint with the Internet Crime Complaint Center at www.ic3.gov.