Protecting Children from Cyber Threat Actors Targeting Student PII

Why are Threat Actors Targeting Students?

Recent data trends have shown that school systems and individual student accounts are being targeted by threat actors at a disproportionate rate compared to other agency types. The Personally Identifiable Information (PII) of employees and students at schools impacted by cyber attacks has become a lucrative target for threat actors. PII is more valuable to a cyber criminal when the owner is a juvenile because juveniles are less likely to notice its loss until they are old enough to access their Social Security Number (SSN) (e.g., purchasing a home, obtaining a passport, employment).

Mitigating the Threat to Students

Parents may consider freezing their child's credit with the three major credit bureaus (Equifax, Experian, and TransUnion) so that it is less exploitable by cyber criminals. Once children are old enough to monitor and utilize their credit, their accounts can be unfrozen.

Children are highly susceptible to online schemes that target their personal information and possible security question answers. 'Social Quizzes' have been trending online and are popular "games" for children to play with their friends. These quizzes involve answering questions such as "what's your favorite color," or "what's your first pets name," and even "what was your first job/car". Answering questions such as the afore-mentioned quiz prompts lead to many people, not just students, revealing the answers they provide for password recovery which can allow threat actors access to their accounts. Although fun, these quizzes provide a lucrative opportunity for threat actors to obtain PII on students that will not change over time and may remain on internet servers for an indefinite period of time.

Aside from speaking with students about the importance of maintaining their online security and freezing their credit here are a few additional steps you can take to keep their PII secured.

- Implement Multifactor Authentication (MFA) on any accounts created especially for banking.
- Monitor a child's health insurance claim information, it can indicate PII was used to access their benefits.
- Secure or shred physical documents with PII present on them. Threat actors can access a dumpster easier than an unsecured network.

Georgia Department of Education Stance on Protecting PII

The Chief Privacy and Information Security Officer for the Department of Education stated the following with regards to protecting student PII:

“There are several reasons why it is important to protect student personal identification information (PII).

First and foremost, protecting PII helps to prevent identity theft and other types of fraud. If a student's PII is compromised, it could be used to access their financial accounts, steal their identity, or commit other types of fraud using their name and other identifying information. This can have serious consequences for the student, including financial loss and damage to their reputation.

Second, protecting PII helps to maintain privacy and confidentiality. Students have a right to privacy and the protection of their personal information. When PII is not properly protected, it can be accessed and used without the student's knowledge or consent, which can be a violation of their privacy.

Finally, protecting PII is important for the security of educational institutions and their systems. If a student's PII is compromised, it could be used to gain unauthorized access to a school's systems or to carry out other types of cyberattacks. This can have serious consequences for the school, including financial loss, damage to its reputation, and disruption to its operations.

Protecting student PII is important to ensure the safety, privacy, and security of both individual students and educational institutions.”