A Lesson in Cybersecurity

The Importance of Securing Schools in the Digital Age

While technology was present in the classroom for years prior, schools became wholly dependent on it overnight in 2020. While in-school learning has returned, the utilization of technology is here to stay. With the use of technology, though, comes its risks. Instead of locked doors and secure filing cabinets, sensitive school information leaves those four walls on a daily basis. With that in mind, hackers often target schools due to the industry's limited budgets, lax protocol, and competing priorities. These increased vulnerabilities can lead to successful cyberattacks, impacting students and administrative staff.

The Threat at Hand

According to research in the last year:

Education: #6 in the top share of attacks by industry from 2018-2022.

Top two most common infection vectors:

- Misusing applications
- Sending malicious email attachments.

IBM

Education: #11 in the top global industries targeted in 2022.

M-Trends

Education: #8 in the top number of incidents and #8 in the top percentage of incidents that became successful breaches.

Common attack tactics:

- Maliciously using of web applications
- Manipulating people to give up confidential information
- Deploying ransomware, holding data hostage.

Verizon

Protecting students and staff against school closures, immense recovery costs, and increased cyber insurance premiums is crucial. The release of personal information, though, has the longest-lasting effects. Hackers often hold data hostage and turn it into random letters, numbers, and symbols, so the victims can't retrieve or read it. This data may include or involve personal information, mental health records, or financial records. When they do so, they often share it online or auction it off on the Dark Web, making students' and staff's personal information vulnerable. This experience can impact their lives much longer than a temporary school closure.

These experiences are unfortunately familiar for school districts such as:

- Baltimore County Public Schools, in November 2020
- Albuquerque Public Schools, in January 2022
- Los Angeles Unified School District, in September 2022
- Minneapolis Public Schools, in March 2023

For BCPS, network upgrades and recovering from damages cost them **nearly $10 million**, all because of an email that looked trustworthy, but wasn't. The hackers were planning their attacks on BCPS and LAUSD for two to five weeks before internal staff noticed the intrusions.

Five Tips to Keeping Threats at Bay

So, what can you do to prevent these cyberattacks? Threat actors must be prevented from lurking on your systems and impacting the lives of students and staff. **Here are our top five tips:**

TIP #1

Educate students and staff on cybersecurity best practices

TIP #2

Limit access to sensitive information to those who need it, only when they need it

TIP #3

Establish guidelines for the secure use of mobile devices that access school resources

TIP #4

Ensure strong security measures for online learning platforms

TIP #5

Develop a plan for if and when a security incident occurs

You Partner in Protection

As a managed service provider, we provide IT and cybersecurity services to a variety of businesses, including those in the education industry. We are backed by an elite, 24/7 security operations center that provides us with visibility, around-the-clock protection, and intel to drive best practices. Together, we can ensure hackers don't linger in your school's cloud environment. Harness our experience protecting schools to better defend you and your students.

Get started today by contacting me via phone or email.

AccuTech™ International

866-248-0250 | info@accutech.com | accutech.com