

# K-12 Cybersecurity: 7 Ways to Protect Your Valuable Data

**K-12 school systems hold an abundance of data, making districts vulnerable to the risk of a cyberattack.**

Cybersecurity firm SonicWall reported a 275% rise in ransomware attacks on K-12 targets in 2023,<sup>1</sup> with the cost of downtime to U.S. education amounting to \$35.1 billion over the last five years.<sup>2</sup>

Yet, a recent Nationwide Cybersecurity Review (NCSR) survey shows that K-12 schools allocate an average of 8% or less of their IT budget to cybersecurity.<sup>3</sup>

With limited resources, how can districts protect their valuable data? Here we offer seven tips for strengthening your defenses.

## 01. **Have a plan.**



A well-thought-out security policy is an essential starting point for preparedness. In the event of a breach, an incident response plan enables you to respond to an attack based on a reliable and tested framework. Planning ahead puts you in a stronger position to contain the damage in the event of an attack.

## 02. **Budget for network protection.**



Investing in data protection may include shielding your information from ransomware and other malware with behavior-based detection software. Firewalls, supplementary email security, and encrypted data storage/backup systems also provide coverage against breaches, like phishing attacks.

## 03. **Require multi-factor authentication (MFA).**



MFA requires users to provide two or more verification methods to gain access to an online account. Requiring the additional step(s) to log in can reduce your risk of unauthorized access by up to 99.9%, according to Microsoft.

## 04. **Use the cloud.**



Storing your data in the cloud is more secure than maintaining your own hardware or keeping your data on paper. Cloud providers must stay compliant with ever-changing requirements, investing in security research, innovation, and protection beyond what a school district could provide.

05.



## Establish technology protocols.

It's vitally important to understand the technology your staff is using. Ensuring all school-related tools and applications are district-approved can prevent security gaps that weaken the protection of valuable data. That includes establishing protocols for using AI tools like ChatGPT to ensure personally identifiable information (PII) isn't compromised.

06.



## Conduct cybersecurity training.

Awareness is the key to prevention. Educating teachers and staff on common ways cybercriminals gain access to networks fortifies your protection. Improving awareness of tactics like phishing emails, for example, can prevent valuable data from being compromised.

07.



## Communicate with students and families about cybersecurity.

Students and families play a role in data security and privacy, too. In a report from the Center for Democracy and Technology (CDT), 72% of parents indicated they trust a school with data, but only 43% said schools had shared how it's protected. Communicating your district's security measures can help reinforce efforts to keep student information secure.

To learn more about ways to strengthen your data security, watch the On-Demand Webinar, [Lock Down Your Data: Cybersecurity Quick Tips](#).