GUIDE

Stay a step ahead of cybersecurity threats in K-12 education

Spectrum BUSINESS®

The digitization of K-12 education, including widespread internet access and the increased use of mobile devices, online learning and smart classroom tools, helps schools reach their goals. Use of Internet of Things (IoT) devices such as sensors for energy conservation and security can help schools and districts contain costs and streamline management. While these important changes enhance teaching and improve operations, they also expand the attack surface for cybercriminals.

Education is a fast-growing target of cyberattacks, and district IT leaders agree that current levels of investment in protection are not keeping up with the growing threat. Only 10% of IT leaders in education feel that their teams are fully staffed.[1]

Lean budgets, aging network infrastructure and the growing sophistication of cybercriminals have driven up the number of attacks year over year. IoT devices are a common vector of choice for cybercriminals, meaning if your school has sensors, smart locks, digital learning tools or other infrastructure connected to your network, you may be at higher risk.

Furthermore, the ongoing digital collection and aggregation of student and staff data is extremely attractive to cybercriminals. In 2024, 116 U.S. K-12 school districts experienced a ransomware attack, a 158% increase from just two years earlier.[3]

To change their risk profile, K-12 schools and districts need to adopt new network security practices.

$1.8M

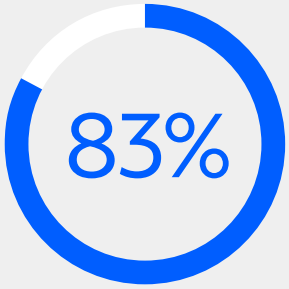
The number of records affected by ransomware attacks on the education industry in 2024.[2]

Tracking evolving threats

The profile of threats is concerning. Attacks can lead to expensive breaches that damage reputations and compromise large amounts of sensitive data, while others shut down systems and disrupt daily operations. You can protect your district from attacks that come from a wide range of attack vectors. Understanding current and emerging types of threats can help you put the right protection in place.

Social engineering

This technique is used by cybercriminals to exploit human psychology and trick people into revealing confidential information or performing actions that compromise security. Phishing is one common method, with attackers often impersonating legitimate entities to steal sensitive data or plant malware through malicious files or downloads. The use of phishing and other social engineering tactics has risen steeply worldwide in recent years.[4]



of phishing emails use AI technology in some form.[6]

AI-powered cyberthreats

These emerging methods leverage AI to create more convincing and automated attacks, making them harder to detect and potentially more effective. One example includes using AI to develop deepfakes, which are realistic fake videos, audio or images employed to trick individuals into granting access to systems or data. AI can also help generate highly personalized phishing emails, power chatbot phishing efforts and attack AI systems by corrupting training data or finding vulnerabilities in the models. On average, 16% of data breaches involve attackers using AI, most often for AI-generated phishing (37%) and deepfake impersonation attacks (35%).[5]

Ransomware and other malware

Malware is broadly defined as any malicious software designed to harm or exploit computer systems. Ransomware is a type of malware attackers use to restrict access to a computer system or files and then demand payment for their release. In 2024, the average ransom demand in the education industry was $847,000.[7] Downloaders are another common malware type, distributed through malicious or compromised websites, typically via fake software updates. New malware variations appear each year, underscoring the need for organizations to remain up to date and vigilant.

Distributed denial of service (DDoS) attacks

These brute-force attacks are throwing more traffic at networks than ever before, combining volumetric, session-exhaustion and application-layer attack vectors. In session-exhaustion attacks, the firewall is essentially turned inside out, becoming a tool for attackers instead of a network defense. Application-level attacks target the code that runs the website or application. In May 2024, over 24,000 students in a Texas school district had mandatory state testing disrupted by a DDoS attack allegedly initiated by a student from his school-issued computer.[8]

$3.8M

The average cost of a data breach in the education industry as of 2025.[10]

Data breaches

The unauthorized access, disclosure or loss of sensitive, confidential or protected information continues to be a risk faced by organizations large and small across industries. The theft can involve personally identifiable information (PII), such as Social Security numbers (SSNs), bank account details and health information, as well as corporate data like customer records and financial information. For example, an attack on Minneapolis Public Schools disrupted learning at multiple of the district's schools and resulted in PII of more than 100,000 people being posted online.[9] In some cases, attackers prefer to corrupt rather than steal from school databases: deleting database tables, changing records or erasing entire databases.

How cyberattacks can be prevented

Breaking down the details of K-12 cybercrimes helps to paint a clear picture of the evolving threat. Consider how the schools in the hypothetical examples below might have been better protected against an attack.

Ransomware attack takes down school website

Type of breach: Ransomware

What was lost: Email, lunch payment services and the school's website were incapacitated; the ransom was paid in bitcoin after six days, but the hackers didn't release the files for weeks afterward. All the district's computers were also unusable during that time.

What might have mitigated or thwarted the attack: Multi-factor authentication (MFA) and segmented security zones within the network could have hindered bad actors from moving laterally if they gained access to one device, while endpoint security solutions could help protect individual devices connected to the network. Use of antivirus software and a next-generation firewall, as well as content scanning and filtering on mail servers, could have protected critical data and prevented intrusion.

Third-party app allows entry into school's computer system

Type of breach: Phishing

What was lost: A hacker sent emails to employees of a third-party medical-benefits vendor, and one staffer responded. As a result, personal information about employees of an entire school district — including full or partial SSNs for about 600 school employees, along with addresses and birth dates for all — was compromised.

What might have mitigated or thwarted the attack: Use of anti-malware protection and a next-generation firewall may have prevented the attack. Encrypted data, both in transit and at rest, would have rendered all the district's PII as unreadable. Use of MFA, updated software and expert training for employees about current phishing methods could have frustrated the attacker's efforts.

DDoS attacks shut down 50 school districts

Type of attack: Volumetric DDoS

What was lost: The technology services center for 50 school districts was shut down nine times during a six-month period by DDoS attacks. Students and teachers lost access to educational materials, officials had to devote significant resources to addressing the attacks and roughly 25,000 students were unable to take the state English assessment tests.

What might have mitigated or thwarted the attack: DDoS protection security services could have blocked the offending IP address and prevented secondary attacks. Machine learning and AI might have identified anomalies in traffic flows, triggering targeted IP-address cleansing. With the address blocked, clean traffic would be allowed to pass, which would have enabled sites to continue operations. In addition, access to a cloud-based portal may well have provided the real-time traffic visibility, insights, analytics and in-depth reporting needed to help avert the attack or limit its impact.

Finding the right protection for your school or district

Continuously keeping ahead of cybersecurity threats to your network requires comprehensive and coordinated coverage. A unified security approach integrated with your internet and network connectivity can help you eliminate vulnerabilities and expedite issue resolution. The approach should include firewalls, unified threat management (UTM) and DDoS protection. The support of a network services provider is also vital, including for cloud-based security services such as secure web gateways, cloud access security brokers, identity management and zero trust network access.

When it's time to evaluate a provider and its services, ask the following questions to help you find the best protection possible:

- How can you protect us from malware, phishing and other common cyberattacks?
- How do you identify and mitigate network threats? Can you scan our network for attacks and drain suspicious traffic?
- What protection do you provide against volumetric DDoS attacks?
- Do you have a means for enabling us to continue to work productively on unaffected parts of the network after a DDoS attack?
- Do you provide UTM? What protection does that provide?
- Can your firewall protect traffic across our various sites?
- Is a next-generation firewall part of what you offer? What does it provide?
- Do you have an integrated solution that includes firewall, UTM and internet service to simplify protection?
- Does your solution provide complete visibility across network components to make potential vulnerabilities easier to identify?
- Can you help implement a zero-trust network architecture with MFA, access management and cloud security for staff working on-site and remotely?
- How are you prepared to support our organization as our network needs change and cyberthreats evolve?
- How can you help offload day-to-day administration work from our IT team during and after implementation?
- What types of teams and experts will we have access to for support? Are they available 24/7?
- How will you ensure all of our WiFi sites are protected?

Comprehensive coverage and support

Widespread, coordinated network protection coverage can keep you one step ahead of evolving cyberthreats in K-12 education. You can balance the needs for complexity in coverage and simplicity in operation by choosing managed security services. With the right partner, you're supported from design through implementation and provided with ongoing support. See how Spectrum Business®, a Charter Communications brand, is uniquely qualified to protect your district's network.

Learn more

1. Amy McIntosh, "Survey Reveals Top Cybersecurity Issues in Education," EdTech, June 10, 2024.
2. Rebecca Moody, "Ransomware Roundup: 2024 End-of-Year Report," Comparitech, January 9, 2025.
3. Luke Connolly, "The State of Ransomware in the U.S.: Report and Statistics 2024," Emsisoft, January 9, 2025.
4. "Global Cybersecurity Outlook 2025," World Economic Forum, January 13, 2025.
5. "Cost of a Data Breach Report 2025: The AI Oversight Gap," Ponemon Institute and IBM Security, July 2025.
6. "Phishing Threat Trends Report," KnowBe4, March 2025.
7. Moody, "Ransomware Roundup."
8. Christian Terry and Bryce Newberry, "Texas Student Uses School's Computer for Cyberattack, Disrupting District Testing for 24,000," Click2Houston, May 29, 2024.
9. Joe Warminsky, "Minneapolis School District Says Data Breach Affected More than 100,000 People," The Record, September 6, 2023.
10. "Cost of a Data Breach Report 2025."