

Protect your K-12 network from cyberthreats

The pressure to modernize and meet the needs and expectations of students, faculty, staff and parents is driving K-12 schools and districts to embrace new technology — including Internet of Things (IoT) devices, online learning and smart classroom tools. These innovations can enhance teaching and improve operations but expand the attack surface for cybercriminals and make schools more vulnerable.

Understand why K-12 is at risk

Schools and districts can be a target due to their large attack surface, the amount of personally identifiable information (PII) they collect and limited funding for cybersecurity.

88%

of public schools have a 1-to-1 computing program that provides every student a school-issued device.¹

1.8M

records were affected by ransomware attacks on the education industry in 2024.²

90%

of IT leaders in education do not consider their teams fully staffed.³



Track the evolving threat profile

The threats targeting K-12 organizations are constantly changing as hackers develop workarounds to gain entry to systems and bypass security responses. Top threats affecting schools and districts include:

- ☒ **Social engineering**
Phishing attacks impersonate legitimate entities to steal data. The use of phishing and other social engineering tactics has risen steeply in recent years.⁴
- ☒ **AI-powered cyberthreats**
AI is being used to create automated attacks that are harder to detect and thwart. Nearly half of organizations worldwide consider the advance of adversarial capabilities to be the biggest security concern surrounding AI.⁵
- ☒ **Ransomware and other malware**
Attackers increasingly use malware that encrypts critical data to bring operations to a standstill before extorting payments. In 2024, the average ransom demand in the education industry was \$847,000.⁶
- ☒ **DDoS attacks**
Volumetric attacks can be executed with tools purchased on the dark web for as little as \$30 per month, making them a frequent threat.⁷ Efforts to overwhelm school networks continue to grow in size and sophistication.
- ☒ **Data breaches**
Unauthorized access or use of confidential data remains a risk for K-12 schools and districts. The average cost of a data breach in the education sector was \$3.8 million as of 2025.⁸

Know where you're vulnerable

Three types of K-12 data often breached:

Student records

PII is the most common type of data stolen or compromised.⁹

Financial and operational data

The number of K-12 districts impacted by ransomware more than doubled from 2022 to 2024.¹⁰

Email and communications

In 2025, research found that K-12 schools faced a 95%-98% probability of an email phishing attack within the next 12 to 18 months.¹¹

Find comprehensive coverage and support

Widespread, coordinated network protection can keep you one step ahead of evolving K-12 network threats.

Discover how you can help safeguard your systems, students and staff with security solutions from Spectrum Business®, a Charter Communications brand.

[Learn more](#)

1. [“More than Half of Public School Leaders Say Cell Phones Hurt Academic Performance,”](#) National Center for Education Statistics, February 19, 2025.
2. Rebecca Moody, [“Ransomware Roundup: 2024 End-of-Year Report,”](#) Comparitech, January 9, 2025.
3. Amy McIntosh, [“Survey Reveals Top Cybersecurity Issues in Education,”](#) EdTech, June 10, 2024.
4. [“Global Cybersecurity Outlook 2025,”](#) World Economic Forum, January 13, 2025.
5. Ibid.
6. Moody, [“Ransomware Roundup.”](#)
7. Michael Hill, [“DDoS Attack-for-Hire Services Thriving on Dark Web and Cyber Criminal Forums,”](#) Cyber Security Hub, December 4, 2023.
8. [“Cost of a Data Breach Report 2025: The AI Oversight Gap,”](#) Ponemon Institute and IBM Security, July 2025.
9. Ibid.
10. Luke Connolly, [“The State of Ransomware in the U.S.: Report and Statistics 2024,”](#) Emsisoft, January 9, 2025.
11. Mike Sanchez, [“How Schools Can Strengthen Cybersecurity in 2025,”](#) UDT, March 19, 2025.