INFOGRAPHIC

Is your K-12 network safe from DDoS attacks?

Distributed denial of service (DDoS) attacks are designed to flood and overwhelm a school or district's internet connectivity to block access to online resources. Attacks can cost schools and districts significant time and money, in addition to lost community confidence. Yet, many schools underestimate the chance of attack.

Fewer than half (48 percent) of ed-tech leaders say DDoS attacks are a medium or high risk for their networks,[1] however...

K-12 schools are an increasingly popular target of attacks

350%

Increase in DDoS attacks in education during the first half of 2020 alone.[2]

120,000+

Number of known DDoS incidents in education in 2020.[3]

24%

Increase in the average duration of a DDoS attack during the first quarter of 2020.[4]

K-12 networks are targeted to:

- Disrupt scheduled activities, such as online assessments.
- Overload a network and prevent access to school applications, systems and information.
- Hinder parent access to school or district online portals.
- Prove it can be done, which is especially easy when school networks lack protection.

Reasons DDoS attacks are on the rise in K-12 schools

Increase in usage of internet-connected devices.

The move to cloud-based applications has created more opportunity for hackers.

More unsecure connected devices make it easy to launch attacks.

The shift to remote instruction during the pandemic put more devices in students' hands.

Lack of protection.[5]

23%

K-12 schools in 2020 with at least one full-time staff member dedicated to ensuring network security.

37%

K-12 schools that did not purchase cybersecurity-related products in 2020.

Simplicity and access.

- With the right tools, DDoS attacks are affordable and easy to execute.
- Instructions for initiating an attack are readily available online.

$10/hour

DDoS attacks sell for as low as $10 per hour on the Dark Web.[6]

Implement a security strategy that includes DDoS protection

To prevent disruptions to the learning process and protect student and faculty data, DDoS mitigation measures need to thwart attackers and prevent network downtime. An ideal solution will:

Monitor and evaluate
Offer your school or district comprehensive traffic evaluation that uses advanced analytics to identify anomalies indicating an attack.

Provide fast resolution
Quickly and automatically detect, redirect and mitigate malicious traffic, minimizing the impact of attacks to your school or district network.

Offer continuous support
Always available 24/7/365 network and security experts for swift issue resolution.

Be prepared, but don't go it alone. A network services provider is uniquely positioned to provide the DDoS protection you need.

Discover how DDoS Protection from Spectrum Enterprise can help protect your school or district network.

LEARN MORE

Sources

1. "The State of EdTech Leadership 2021 Survey Report," Consortium for School Networking (CoSN), 2021.
2. "DDoS Attacks on Virtual Education Rise 350%," Infosecurity Magazine, Sept. 4, 2020.
3. "Easy and Inexpensive, DDoS Attacks Surge in Higher Education," EdTech Magazine, May 21, 2021.
4. "DDoS Attacks Surge in Size, Frequency and Duration," Security Intelligence, July 30, 2020.
5. "The State of EdTech Leadership 2021 Survey Report," Consortium for School Networking (CoSN), 2021.
6. "The Dark Web: DDoS Attacks Sell for as Low as $10 Per Hour," Mission Critical Magazine, Aug. 26, 2020.

Spectrum ENTERPRISE