

# Is your campus network safe from DDoS attacks?

A distributed denial of service (DDoS) attack can cause significant disruption to the network, applications or services your institution relies on. This can adversely affect your operational and educational capabilities, in addition to being potentially costly and impacting your institution's reputation.

## Colleges and universities are popular hacker targets

**3,574**

The number of weekly cyberattacks experienced by the average educational organization.<sup>1</sup>

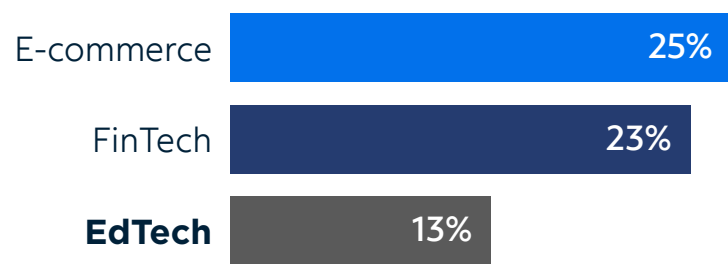
**75%**

The increase in the average number of weekly attacks per education organization from 2023 to 2024.<sup>2</sup>

## DDoS threats are expanding

Today's large-scale DDoS attacks are designed to flood and overwhelm a college or university's internet connectivity, preventing access to online resources for students, faculty, staff and alumni. Cybercriminals exploit institutions with limited cybersecurity budgets, a shortage of dedicated cybersecurity staff and outdated security technologies.

### Top three DDoS targets<sup>3</sup>



**549%**

The increase in web DDoS attacks from 2023 to 2024.<sup>4</sup>

**10,963**

The number of network-layer DDoS attacks the average organization experienced in 2024.<sup>5</sup>

## Goals of attacks on campus networks

- Extort institutions for a ransom to stop the attack.
- Interrupt time-sensitive scientific research data collection.
- Disrupt scheduled activities or cause chaos.
- Overload a network and prevent access to educational tools and information.
- Hinder online collaboration among students or with external sources.
- Prove it can be done, which is easy when an institution's networks lack protection.

**\$6,130**

Average cost of an application-layer DDoS attack per minute.<sup>6</sup>

## Reasons DDoS attacks are on the rise in higher education



More unsecured connected devices makes it easy to launch attacks.



The proliferation of Internet of Things (IoT) devices has expanded institutions' attack surface.



Inadequate resources complicate a school's ability to fend off attacks.



Easy access to affordable DDoS tools and instructions online simplifies attacks.

**\$30 a month**

The cost of a subscription for DDoS attack-for-hire tools on the dark web.<sup>7</sup>

**174%**

The increase, noted by one platform in a single month in 2024, in the use of botnets, a key component of many DDoS attacks.<sup>8</sup>

## Implement a security strategy that includes DDoS protection

To prevent disruptions to your network and safeguard your campus, DDoS mitigation measures need to thwart attackers and prevent downtime. An ideal solution will:



### Monitor and evaluate

Offer intelligent monitoring and comprehensive traffic evaluation that uses advanced analytics to identify anomalies.



### Provide fast resolution

Quickly and proactively detect, redirect and mitigate malicious traffic, minimizing the impact of attacks.



### Scale with needs

Easily and seamlessly expand the solution as the demands of your institution change.



### Offer continuous support

Provide always-available network and security expertise for swift issue resolution.

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

Discover how DDoS Protection from Spectrum Business® can help safeguard your network.

[Learn more](#)

1. "The State of Cyber Security 2025," Check Point Research, 2025.

2. Ibid.

3. "Q1 2024 DDoS Attack Statistics and Overview," QRator Labs, May 20, 2024.

4. "2025 Global Threat Analysis Report," Radware, 2025.

5. Ibid.

6. "Application Security in a Multi-Cloud World 2023," Radware, November 8, 2023.

7. Michael Hill, "DDoS Attack-for-Hire Services Thriving on Dark Web and Cyber Criminal Forums," Cyber Security Hub, December 4, 2023.

8. "Cyber Threat Trends Report: From Trojan Takeovers to Ransomware Roulette," Cisco, June 2024.