As Distributed Denial of Service (DDoS) attacks on campus networks become increasingly common, higher-education technology leaders should consider investing in a solution that safeguards their networks from these debilitating attacks.

A DDoS attack occurs when a hacker takes control of several computers and aims them at a single server, overwhelming that network with traffic and ultimately knocking it offline. DDoS attacks can be very disruptive to teaching, learning, communication, and other day-to-day operations at colleges and universities.
Safeguarding Campus Networks from DDoS Attacks

Anyone can go on the dark web and find instructions on how to launch a DDoS attack.

Because DDoS attacks are fairly easy to execute, the number of colleges and universities that have experienced them is on the rise. Here are some recent examples:

- After four DDoS attacks during the 2014-15 school year, Rutgers University spent $3 million to upgrade its network security. But these upgrades reportedly failed to protect the university from yet another attack in fall 2015.

- Arizona State University experienced a significant DDoS attack in April 2015 that targeted several critical web pages and the university’s internal portal for students, faculty, and staff, MyASU. These resources were down for about eight hours before service was restored.

- The University of Georgia was the victim of a DDoS attack last year that disrupted internet service for students and staff for several hours.

One reason colleges and universities are seeing a rise in DDoS attacks is because more and more students are capable of executing such an attack. Anyone can go on the dark web and find instructions on how to launch a DDoS attack, and the bandwidth needed to do so is fairly inexpensive. Some students are launching DDoS attacks on their own institutions because they are upset with a grade they received, or they want to postpone an exam they feel unprepared for.

But DDoS attacks aren't simply a nuisance; they can be used to hide other criminal activity as well.

A hacker could be using a DDoS attack to hide the fact that he or she is trying to install a virus on the network, for example—or break into the network to access Social Security Numbers, credit card data, or other information.

While there are premise-based solutions that can shut down a network in the event of a DDoS attack, the best option is to implement a cloud-based solution that can intercept the barrage of traffic attacking the network before it even reaches its intended server. That way, colleges and universities are not affected by the attack; the additional traffic is diverted from their network, where it is analyzed to determine who is doing the attacking.

DDoS Defense from AT&T is one such solution. It detects the presence of a DDoS attack in near real-time and diverts offending traffic to scrubbing facilities, while allowing the flow of legitimate communication.

To learn more about how AT&T can help your institution protect & respond to cybersecurity threats, visit att.com/edu or contact an Education Specialist for additional details.

© 2017 AT&T Intellectual Property. All rights reserved. AT&T and the AT&T logo are trademarks of AT&T Intellectual Property.