SHARDSECURE

DATA PROTECTION FOR HIGHER ED

When it comes to data security, colleges and universities face unique challenges. Individual departments may use a wide variety of legacy IT systems, and bring-your-own-device (BYOD) environments offer myriad entry points for attackers.

Luckily, you don't have to be a computer science scholar to protect your students, staff, and campus from data security threats. Our guide explains how to safeguard against the top six threats in higher ed.

Reduce your attack surface

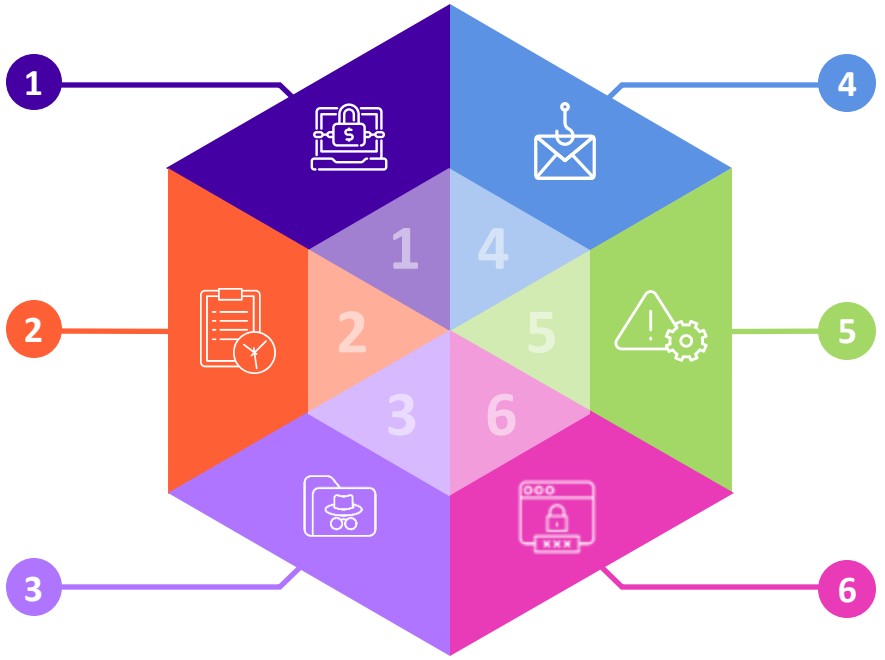
Colleges and universities have unusually large attack surfaces. With a high number of student and faculty devices, plus a wide variety of websites maintained by individual professors or departments for educational purposes, schools offer thousands of entry points for attackers. To minimize this attack surface, IT teams should be sure to segment networks, monitor endpoints, and decommission unused webpages.

Update, update, update

Having the latest web browsers, operating systems, and security tools is surprisingly crucial for data protection. Ensure that faculty, staff, and students are regularly updating any laptops, mobile phones, and other devices that will be accessing the school's network.

Protect against ransomware

Studies show that 64% of higher ed institutions were hit by ransomware in 2022, costing well over $3 billion in downtime alone. Some schools have had to rebuild their core systems from scratch, and one even closed permanently. To avoid significant damages, institutions should invest in strong data security solutions, including anti-malware software and backup services.



Teach students and staff about phishing

Phishing attacks can target even the most tech-savvy with increasingly sophisticated forms of social engineering. To avoid attackers gaining access to sensitive information like passwords and financial information, offer campus-wide training on phishing. Teach users never to click on suspicious links, download unknown attachments, or respond to unsolicited phone calls, text messages, emails, or DMs with personal details.

Avoid outages

Losing access to critical networks for even a day can significantly disrupt teaching, student life, and campus operations. Universities must implement robust data resilience solutions to ensure high availability and avoid costly downtime.

Keep records confidential

Data privacy and confidentiality are essential for colleges and universities. Everything from student grades, medical records, and financial aid packages to admissions files and staff payroll must be kept private to ensure safety. Learn how ShardSecure renders confidential information unreadable to unauthorized users with its innovative, easy-to-implement approach to data protection.

Ultimately, the data security threats facing your campus may be as varied as your student body. But with the right knowledge and tools, colleges can protect themselves against the most common and devastating attacks. To learn more about how the ShardSecure platform mitigates cloud ransomware, outages, and data breaches with advanced data security and resilience, visit our resources page.