CyberloQ

Higher educational institutions are now prime targets for hackers worldwide.

It's time for colleges, universities, and trade schools to pay attention.

Think of all the valuable information cyber criminals would like to get their hands on: Private student information, proprietary research, and a plethora of financial data.

And the pressures are rising: With funding and resource crunches facing IT staff, plus increasing regulations on internal data security like NIST 800-171, FERPA, and HIPAA, protecting the Personally Identifiable Information (PII) of students is a pressing concern now more than ever.

With the average value of a student's personal data record being around $200, hacking colleges and universities is becoming increasingly lucrative. Cyber criminals recognize the IT and cyber security departments at many higher learning institutions are fragmented, lacking resources, and lagging in cyber defense.

In 2017:

455 reported cyber security incidents **in the educational sector**

73 incidents resulted in **data disclosure**

Verizon's 2017 Data Breach Investigations Report

Cyber-attacks and data breaches don't just cost universities valuable time and money to assess the damage and mitigate losses – They can be a serious reputational blow that will affect future enrollment in both the short and long term.

Higher educational institutions of all shapes and sizes need to take a strong, aggressive, proactive approach to cyber defense with a cutting-edge partner like CyberloQ.

CyberloQ

1.833.292.3757
info@cyberloq.com
www.cyberloq.com

Secure Multi-Factor Authentication

Advanced Credit Technologies' patent-pending CyberloQ™ technology adds one more tool to a higher learner institution's arsenal to fight unauthorized access to protected resources. Rather than simply responding to a data breach, CyberloQ uses Multi-Factor Authentication (MFA) to pro-actively ensure that only authorized users, on approved devices within designated locations, can access your school's protected student, faculty, and administrative data.

Securing a Surveillance Perimeter Around Your Campus

Data protected by CyberloQ can be accessed only by those employees, faculty, or administrators who have been registered with the learning institution's secure CyberloQ enabled database. CyberloQ enabled client accounts will always be in an "inactive" state until the client uses their mobile device (a smartphone, laptop or tablet) and PIN, functioning as part of a multi-factor authentication system that is required to access any protected information. Universities can also use CyberloQ's administrator-defined geofencing capability to ensure that the user/device is within a specified geographical perimeter before access is granted. This location can be as large as a city or, using physical beacons, as small as a room, providing the ultimate perimeter surveillance scalability. If a hacker breaches the perimeter of the geofence, the account and access is automatically disabled. This feature puts our system apart from the rest in a world where university data are increasingly accessed via "always-on" active accounts.

Iron Clad Educational Security

We're currently developing enhancements to add additional layers of security to CyberloQ's current multi-factor authentication solution by including biometrics for the highest level of access security.

By using CyberloQ's multi-factor protection technology, institutions of higher learning can be prepared to meet emerging cybersecurity standards, regulations, and guidelines that will be required to maintain federal funding and grants. Data records are recorded in a global administrative console that is easily accessible to university IT staff or administration at any time, and these records will become essential in proving compliance with new regulations.

Grounded in 30+ years of experience providing domestic and international cybersecurity services for the Government, our patent-pending CyberloQ™ technology is designed specifically to provide a solution for proactive, real-time control of identity governance to protect any institution of higher learning's valuable and private student records, academic data, and administrative information.

Global View Console

Featuring comprehensive details and reporting for each information activation across users, devices, and locations.

- **GPS and Location Reports**
- **User Tracking Reports**
- **History Reports**
- **Activation Calendar**
- **Activation Map**

Mobile App
Supports GPS and Location Permissions