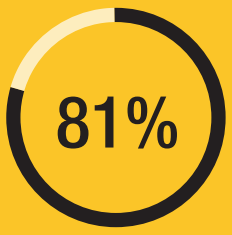
of all security breaches take place in higher education

is the average cost of a higher education data breach



of data breaches are due to weak, default or stolen passwords

Higher education is learning the hard lessons of cyber theft

Higher education is just as vulnerable to data breach as retail, healthcare and the financial sectors. In fact, higher education ranks third among the top 10 most-breached sectors. Motivations behind data theft at higher education institutions are similar to those of other industries. They involve financial gain, personal data exposure, and intellectual property theft. In addition to a tarnished image, data breaches have a significant financial impact on colleges and universities. Costs related to data breach expense can include forensic consultants, lawyers, call centers, websites, mailings, identity-protection, credit-check services and litigation. The average cost of just one higher education record breach is $142 and can be as high as $300 per record quickly adding up to millions of dollars of exposure in a single cyber attack. So how do we prevent higher education cyber crime?

The greatest risk of breach can be isolated to the most basic of security concepts, the “password”

It is well-documented that passwords pose the greatest security risk to organizations today; Verizon reported over 81% of data breaches are due to weak employee passwords. In addition, 65% of U.S. adults use the same password for all of their accounts. The largest security gap in higher education can be closed with strong password policies enforced with an easy to use, intuitive password management solution.

Protect your institution and students with enterprise-strength password management

Keeper is the trusted leader in password management helping organizations manage, secure and enforce strong passwords across all employee logins, applications and sites. Faculty, administrators and students can access Keeper natively on all mobile operating systems, desktops and browsers.

Data is protected in Keeper’s *zero-knowledge* security architecture with world-class encryption. Zero-knowledge means that only the user has knowledge of and access to their Master Password and the encryption key that is used to encrypt and decrypt their information. Keeper uses 256-bit AES encryption, which is used to encrypt classified data designated as TOP SECRET by the U.S. Government.

Key Features

- Effective and intuitive password management
- Enhanced protection with two-factor authentication
- Secure file storage and sharing
- Cloud-based, OS and device independent
- Admin console with reporting, auditing and analytics
- Fast deployment with AD/LDAP provisioning
- 24x7 support

Key Benefits

- Mitigate cyber risk
- Maintain regulatory compliance
- Increase employee productivity
- Enforce password policies and procedures
- Reduce help desk costs
- Minimal training, fast time-to-security
- Improve employee security awareness and behavior

For more information contact sales@keepersecurity.com or call 312.829.2680

Reduce costs and improve productivity with Keeper

Password resets are a major burden on the productivity of IT departments. The #1 help desk call is for a forgotten password - Gartner estimates the annual industry cost for password resets is around $10B per year.

Keeper provides cost savings to customers by reducing help desk calls and increasing employee productivity. Employee passwords are encrypted and stored within Keeper so employees no longer need to remember them. Keeper auto-fills login credentials across mobile applications and browsers, which greatly improves productivity. If an employee forgets their master password, Keeper allows employees to set a security question so the master password can be recovered without IT assistance.

Finally, all Keeper users have 24x7 access to Keeper's dedicated customer care team. With Keeper, those costly help desk calls will be significantly reduced and the burden of resetting passwords will become a thing of the past for the IT department.

Secure more than just passwords

Passwords are one of many confidential assets that businesses need to secure. Keeper protects your sensitive files, documents, digital certificates, private keys, photos and videos in a highly-secure, encrypted digital vault. You can securely share files with colleagues and have confidence knowing that your information is backed up in Keeper's Cloud Security Vault™.

The Keeper difference

Only Keeper….

- Provides a simple, intuitive and unified password manager and digital vault
- Has an impenetrable security architecture with rigorous 3rd party audits (SOC II Type 2 compliant)
- Delivers native applications across all major devices, operating systems and browsers
- Provides password policy visibility and enforcement
- Has a dedicated customer care team 24x7x365

Who uses Keeper?

Over 3,000 organizations trust Keeper including University of Alabama Birmingham, University of Iowa, Ohio State University, University of Maryland and more.