

RESOURCE CENTER

Safeguarding higher ed data: Why educational institutions must prioritize password management

Get the full interactive view at
<https://bitwarden.com/resources/why-educational-institutions-must-prioritize-password-management/>



Safeguarding higher ed data: Why educational institutions must prioritize password management

Schools and universities are increasingly becoming targets for cyberattacks. Just consider these grim facts:

- Microsoft registered nearly [4.5 million cyberattacks](#) in the U.S. in April, 2023, with 80% of attacks targeting educational institutions, according to the Microsoft Global Threat Activity Tracker.
- Education was the [third most-targeted sector in Q2 2024](#), based on the number of analyzed events.
- Universities are prime targets, facing an average of 2,507 cyberattacks per week, according to a 2023 [report from Check Point](#).
- K-12 institutions are hardly immune. K12 Security Information eXchange (K12 SIX) tracks cyber incidents targeting the U.S. primary education community. They logged [over 1,600 such incidents](#) from 2016 through 2022, with a sharp spike in 2020 and 2021.
- A [record number of ransomware attacks](#) hit schools and universities in 2023, according to Comparitech.
- Monetary losses to school districts range [from \\$50,000 to \\$1 million](#) the U.S. government's General Accounting Office reports.

What's behind this massive surge in activity? Simply put, cybercriminals are taking advantage of the education sector's quick adoption of e-learning.

Unlike retail stores and businesses, which have been operating online for years and have had time to build expertise and a strong security culture, educators had to move to digital platforms very rapidly during the COVID-19 pandemic. That has led to a gap between educational institutions' technologies and their ability to defend them.

Complicating matters: Many students and staff regularly bring their own devices onto the institution's network and are often reluctant to practice basic cybersecurity hygiene.

Add all this together, and you have a perfect storm of vulnerability. Cybercriminals know this, and they've wasted no time in getting to work attacking schools worldwide.

Fortunately, there's a simple step that every educational institution can take to increase their security posture: Implement strong password management.

Why education needs strong password management

[Password management improves organizational security](#), according to a recent survey of Bitwarden users. In educational institutions, it gives users a way to manage scores of passwords securely. Instead of writing them down on pieces of paper stuck to their monitors, users can now store passwords securely in an encrypted vault. And because the passwords can be more easily managed that way, it's far easier for users to give every one of their online services a unique password, which eliminates password reuse — a major vulnerability.

A good password manager can help students and staff create more secure passwords. Rather than using short, easy-to-guess words, the password manager can generate long strings of random letters, numbers, and special characters, which are virtually impossible for hackers to crack. A weak password, with 5-7 characters, can take only seconds to crack. A strong password with 16 or more characters would take centuries.

What's more, a password manager gives a simple, manageable way for educational institutions to share passwords among staff members who need to use shared accounts. With a modern password manager, every user has their own personal vault, where their login credentials are stored in a secure, encrypted form. The organization can also enable shared vaults, which are accessible to specified users. These vaults enable organizations to share login credentials among multiple users securely and with continual oversight.

IT administrators also value the way that password management software helps them implement regular security training and elevate the overall security culture at their organizations. The password manager becomes the focal point of their efforts to promote good security hygiene, reminding people of how important it is to use good passwords and not to reuse the same password with multiple online accounts.

Finally, with a modern password manager, IT managers and end users can get alerts when a user's password appears on a list of compromised passwords. This happens when attackers gain access to a password and share that information on "dark web" marketplaces. If those passwords are being reused, this becomes a major vulnerability, as every service where the user employs that password is now easy for hackers to access.

Additional benefits of strong password management

There are education-specific compliance and security requirements that strong password management can help meet.

Compliance with the Family Educational Rights and Privacy Act (FERPA). This act means educators and school administrators are responsible for keeping student data safe. It's difficult to do that without strong password management.

Securing access to educational platforms. Whatever digital platform your school or university uses, you want to ensure it's as secure as possible. You can only do that if you know users have sound password management. Whether they're using Google Classroom, Canvas, Blackboard, Class Dojo, or another platform, secure access is crucial.

Protecting your student's data. Educational institutions are the guardians of many kinds of personally identifiable information (PII), including names, dates of birth, grades, attendance records, disciplinary records, home addresses, and Social Security numbers. If the systems storing this information aren't secured with strong passwords, all that data is potentially vulnerable.

Secure sharing and collaboration among educators. Teachers and staff often share account logins. Ensuring that they have the ability to do that securely is important. Passing around slips of paper with login details, or sending them by email, opens these accounts to compromise.

Management of both professional and personal accounts. It's not only school accounts that need to be secured. Staff and students alike all have websites and apps they use for personal reasons, and those need to be secured as well. [K-12 students use an average of 72 different apps](#) — how many use the same password?

Bitwarden: The right solution for higher ed

A password manager is the easiest way to create, store, and retrieve strong, unique passwords while reducing susceptibility to social engineering attacks.

For IT security administrators, Bitwarden gives you the ability to control who has access to your critical applications, and facilitate easy and secure sharing of credentials. Create Collections of passwords to allow users — your educators, visiting professors, and administrators — to share items with other members of the same organization. Typically, these will be named based on departments or areas of responsibility. Each member of the organization may have different Collections available to them based on their role.

Educators, teachers, and professors can ensure e-learning applications that facilitate course management, content delivery, and interaction among students are protected by strong and unique passwords secured within an end-to-end encrypted Bitwarden vault. Without strong credentials and multifactor encryption, educators are putting personal information, addresses, educational records, payment details, and intellectual property at risk.

For students, Bitwarden provides a convenient, secure way to store passwords for all the online services you use — not just school-related websites. Install the Bitwarden browser extension and mobile app to make using Bitwarden as convenient as possible — with these, you'll have access to your logins wherever you go.

Bitwarden gives higher ed institutions greater control over their credentials, which improve overall security. For those exploring passwordless authentication, Bitwarden also offers passkey management for all users, and passkey APIs and developer toolkits for developers to easily deploy passkey authentication.

To find out more about how Bitwarden can improve your school or university's security, [start a free 7-day business trial today](#).