LastPass •••|

Password Hygiene in Higher Education

Risks, Solutions, and Strategies.

Table of Contents

Introduction

One of the many lessons learned from the pandemic is that today's higher education IT teams, along with IT professionals from a range of industries, are managing a vast volume of priorities and needs across their institutions. Chief among these priorities:

Protecting the personal information of students, faculty, and staff from digital criminals through proper password hygiene–and finding the right tools to reduce the risks.

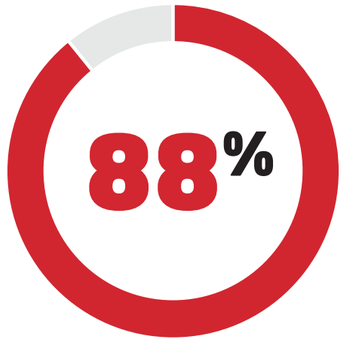
That is no easy task given the copious amounts of data produced and stored by higher education institutions. Complicating matters: an ever-expanding range of devices, applications, and networks that increase the complexity of managing and protecting an on-campus, remote, or hybrid IT environment. Not to mention, a population that spans from tech-averse to tech-savvy, presenting further challenges to safeguarding systems and data.

The challenges of safeguarding systems and data.

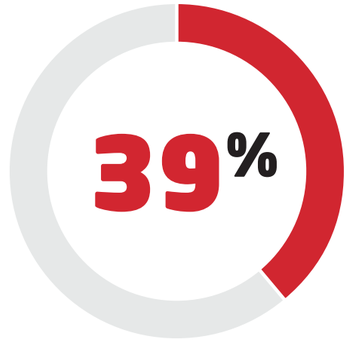
This problem is very real and very present, according to an International Data Group (IDG) survey of 300 IT higher education professionals, sponsored by LastPass.

This paper explores these IDG survey findings and analyzes solutions and strategies to protect critical systems and sensitive data, with additional commentary from subject matter expert, Kim Milford, Executive Director, The Research and Education Networks Information Sharing and Analysis Center (REN-ISAC).

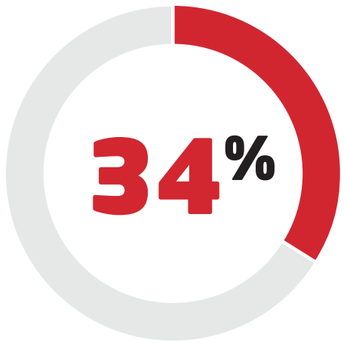
Did you know...



of institutions suffered an IT security infringement because of poor password management this year alone.



of respondents report difficulty keeping up with the latest cyber threats.



are challenged in keeping up with the volume of staff and student changes.

are stymied by protecting every entry point and device accessing the institution's data and applications.

The role of passwords in cybersecurity.

Under resourced IT teams, massive amounts of data, a diverse population of users, an open culture—they are all factors that can increase a higher education institution's exposure to cyberthreats. Central to overcoming these technological and cultural obstacles is password management.

As a growing number of entities—such as healthcare facilities, government agencies, and educational institutions—fall victim to cyberattacks due to poor password hygiene, password management has emerged as a critical component in any IT cybersecurity strategy.

What is password management?

In its simplest terms, password management involves storing, securing, and managing credentials by following a set of principles (e.g., storing your password in a digital vault) and best practices (e.g., never reusing a password) to prevent against unauthorized access to an organization's sensitive data and critical systems.

What higher education IT professionals think about password, identity, and access:

82% Even higher priority than other IT security initiatives

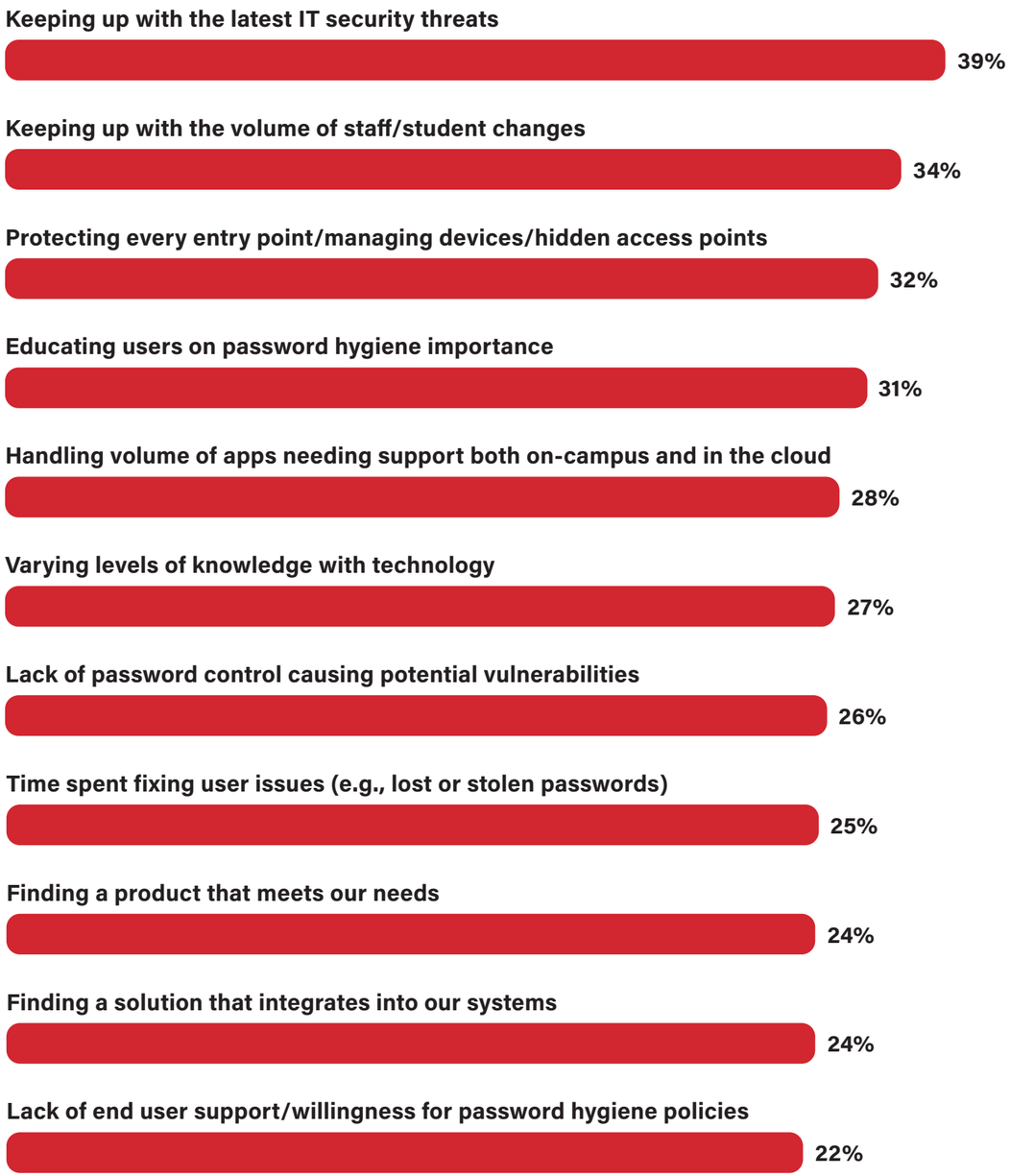
81% Even higher priority than phishing/malware/denial-of-service prevention

79% Even higher priority than data governance/compliance

However, as IT landscapes expand, and passwords proliferate, the need for colleges and universities to embrace stringent password management strategies and solutions becomes imperative in minimizing the risk of cybersecurity breaches.

After all, while passwords are often the first line of defense for students, faculty, and staff, they are also a key target for hackers.

The many challenges of password management.



The risks of poor password hygiene.

Despite increasing awareness of the importance of password hygiene, and the concerns it raises for students, faculty, and staff, there are always more safeguards that can be deployed to better manage passwords and user credentials in today's landscape of rapidly evolving threats.

Because many students, faculty, and staff make the mistake of recycling passwords, stolen credentials can grant hackers immediate access to multiple accounts–a significant challenge for often under-resourced IT teams.

46% **Chief among respondents security concerns is stolen credentials.**

The impact of poor password management to your Institute.

Even the best cybersecurity solutions are put at risk with poor password hygiene.

The reality is that many institutions have invested heavily in cybersecurity solutions, from firewalls and intrusion prevention systems to antimalware software. But if students, faculty, and staff have poor password hygiene habits, it can significantly weaken an institution's overall security posture and hamper efforts to maintain the highest standards of security.

Higher education students, faculty and staff want to be able to trust the institutions that collect and store their most personal data.

61%

Classified their level of risk as "elevated, high, and in some cases severe."

44%

Cited breach of financial and/or personal information as one of the most concerning dangers of poor password management.

42%

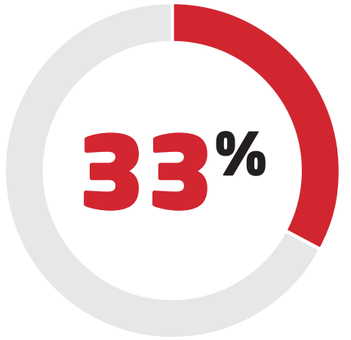
Believe that reputational harm from security incidents is a damaging consequence for their entire institution.

Common errors can be risky.

Contributing to these risks is a wide array of common password user errors, many of which can significantly threaten the security of an institution's overall data integrity and its reputation.

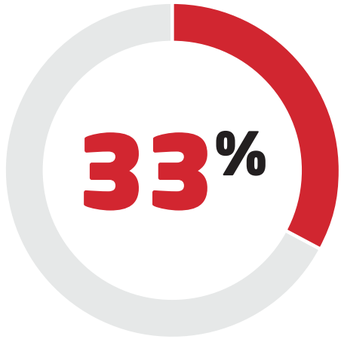
"Students, faculty, and staff, busy with their teaching and learning activities, can at times lose sight of good password hygiene. This puts their personal information at risk and may open doors for bad actors to access sensitive institutional information."

Kim Milford, Executive Director
of the Research and Education Networks
Information Sharing and Analysis Center (REN-ISAC)



Use similar passwords

A single leak of that password could put a user's accounts at risk by enabling a malicious hacker to log into multiple online accounts.



Share credentials

Making it easy for bad actors to access critical systems and other parts of a network.

Rely on weak passwords

Passwords can be easily compromised, creating potential entryways for cybercriminals to steal confidential data and personal information.

Seeking a solution for greater protection.

The good news is that many higher education institutions are aggressively pursuing password management solutions for constituents.

88%

Have at least one solution in place across the entire institution.

73%

Plan to implement new or additional solutions for various cohorts over the next six to 12 months.

53%

Have a solution in place within each individual constituency of students, faculty, and staff.

32%

Have alumni who are using password management solutions.

Prioritizing deployment plans.

Deployment plans and audience priorities for password management solutions tend to vary based on the size of an educational institution and the risk management practices in place. Smaller institutions with limited staff must prioritize the implementation of password management safeguards to the varied audiences based on the risks to institutional data, i.e., staff with access to student information systems are prioritized over students, who have access only to their own personal information.

71% of universities have already deployed solutions for faculty members.

46% of private institutions are slightly slower to deploy solutions for students than for the general public (59%).

71% of smaller institutions are most likely to have a solution in place for staff.

IT teams are largely aligned on the objectives they hope to achieve with a password management solution.

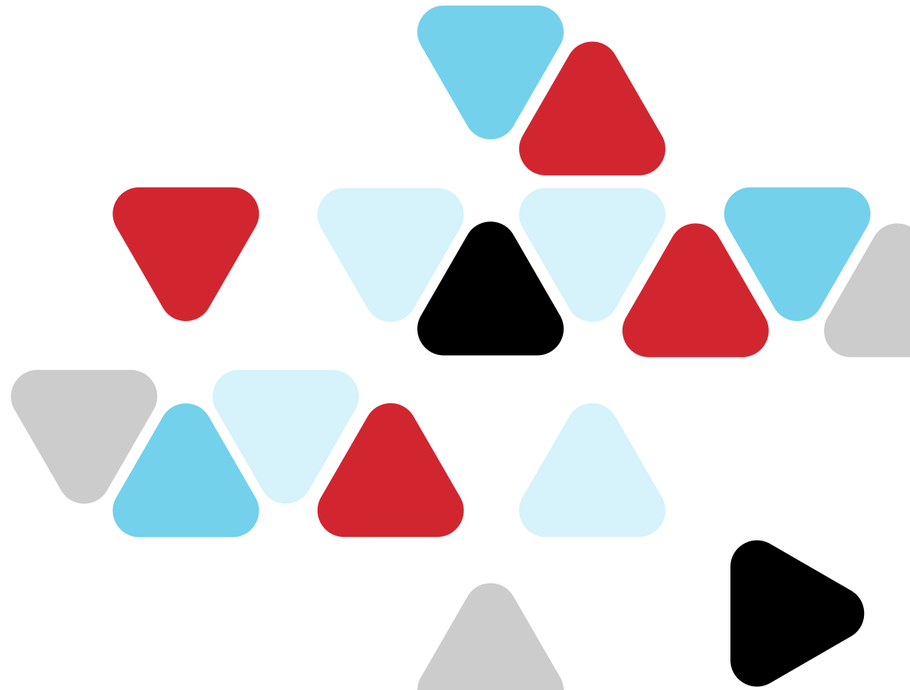
40% of the respondents cited the need to protect sensitive data as the primary driver for deploying, planning, or considering implementation of a password management solution.

34% of the respondents (more than a third) said allowing for secure remote working and learning is a top priority.

Many higher education institutions are welcoming students, faculty, and staff back to campus and classroom facilities. Nevertheless, the pandemic has forever changed expectations of working and learning in a higher education environment. Students now demand flexible learning opportunities that offer both in-classroom and digital-first experiences, and faculty and staff expect flexibility in terms of when and where they work.

29% of IT professionals in higher education are focused on increasing visibility of potential threats.

Meeting these needs not only requires supporting remote access to critical data and systems but doing so in a way that protects sensitive information. Along these same security lines, one-third of IDG survey respondents are looking to password management to enhance their overall security posture.



A global view of password management.

Size and student body aren't the only factors that can influence a higher education institution's password management priorities. Geographic location can also dictate goals and attitudes.

Some of the most interesting regional differences that surfaced in IDG's survey:

- Respondents in APAC are more like to have cited "help with IT modernization efforts" [such as updating IT tools] (31%) as a primary driver for password management.
- APAC respondents consider "overall financial loss" (44%) as one of the most likely negative consequences of poor password management.
- Institutions in the U.S. find managing end user password hygiene slightly easier (66%) than those in EMEA (59%) and APAC (61%).
- "Pressure to find free solutions" is more likely to inhibit the ability to implement a password management solution among institutions in APAC (42%), budgets can be restrictive.
- The higher education administration is more likely to be involved in the evaluation and purchase of password management solutions in the U.S. (54%) and APAC (49%) than in EMEA (29%).

Build a strategy for success.

Fortunately, a password management solution can help by simplifying password management for students, faculty, and staff while providing IT teams with greater visibility and actionable oversight, from advanced reporting tools to customizable security policies.

"While ongoing end-user education continues to be a critical step to any defense-in-depth strategy, password management solutions can support institutional goals robustly. They can be used to reduce risks to passwords, improve user convenience, and allow IT teams to assist their users more effectively," notes Milford.

Not all password management solutions are created equal.

44% Managed multiple password management tools, resulting in a hodgepodge of features and functionalities.

37% Rated managing password hygiene as very or somewhat difficult, posing vulnerabilities to IT security systems and adding to IT headaches.

So, what should higher education institutions look for in a password management solution?

The answer is a combination of administrative and end user ease of use.

The list of must-have attributes narrows as institutions enter the final stages of selecting a password management solution. For example, 75% of respondents report ease of use as a "critical" or "very important" feature when evaluating a vendor's solution. Many higher education institutions have a large and diverse population of users, ranging from those with a digital-first mentality and those who are still adjusting to new tools– and a secure mindset. Higher education institutions demand a password management solution that can cater to varying degrees of comfort and knowledge when it comes to technology and security. This will allow for seamless onboarding and widespread adoption.

IT TEAMS WANT ASSURANCE THAT THE SOLUTION THEY'RE DEPLOYING IS TRUSTED BY PEERS IN ACADEMIA.

Key considerations for institutions include finding a solution that embodies the latest technology (74%), as well as one that is vetted by a trusted third party (74%).

Today's most-sought-after technical features:

27% Integrations with an existing environment

26% Password generator

25% Group management

24% Accessibility from any browser/device

23% Password vault

22% Detailed reporting capabilities

A deep dive into a password management solution.

How can higher education institutions be sure they're selecting a solution that not only offers the best technology features but also allows for ease of use and simple integration?

"Password management solutions can complement institutional policies and identity management practices by improving user convenience, reducing the risks of password reuse and password sharing, and enhance the administration of account terminations and forgotten passwords," according to Milford.

Here's a more granular look at what to consider when assessing password management solutions:

Convenient and simple password storage. Users should be able to generate unique passwords, easily save and fill credentials, and rely on secure and flexible sharing for collaborative teams, from IT to the marketing department—even those external to the institution such as students and alumni—all while maintaining accountability.

Greater control of employee/student hybrid environments. Using an intuitive and centralized administration console, a password management solution can provide IT leaders with greater insight into their working environment and more access control. For example, by using generated passwords and revoking access in real time, IT teams can ensure that critical data doesn't depart each semester along with migrating students, faculty, and staff.

Incentives for solution adoption. Scalable, automated integrations with user directories can simplify employee onboarding and offboarding and allow for automated management. Look for solutions that can be integrated with top identity providers, such as Microsoft Active Directory Federated Services (ADFS), Microsoft Azure AD, Google Workspace, and Okta, to boost security, productivity, and adoption.

Customizable packages to meet varying needs. By offering highly customizable packages, the right solution can accommodate a wide array of IT needs, including a secure password manager for IT teams and collaborative staff departments, as well as personal accounts with secure, private vault functionality that's accessible from any device or browser for students, faculty, and staff.

Accessibility for all. To better serve today's diverse student body, the right password management solution should be able to offer keyboard navigation and updated proper color contrast and readability, as well as region and language tags to enable users to navigate with screen readers and keyboards more easily.

Ease of use for busy IT teams. Reduce IT burden and increase compliance with a modern password policy that's easy to deploy and use. With policy options available in a centralized admin console that align with an institution's policies, IT teams can meet and exceed security goals without adding complexity.

A worthwhile solution.

One solution that offers all these key attributes is LastPass, a password management tool that saves, stores, and organizes passwords and logins in a vault encrypted to ensure security while easing user access and IT workloads.

SURVEY FINDINGS

As IDG survey findings indicate, a single security incident precipitated by a weak or repeated password can easily erupt into a full-blown security breach. That's all the more reason for higher education institutions to deploy a robust password management solution such as LastPass. Not only can it protect sensitive data and support new ways of learning and working but the right solution can also serve as a powerful foundation for greater IT growth. This way, institutions can easily incorporate additional layers of protection, such as multifactor authentication and single sign-on, to an account for an ever-evolving defense against today's sophisticated cyberattacks.

LastPass for higher education institutions.

For more than 1,200 higher education institutions, LastPass helps IT employees, faculty, staff, and students keep credentials safe across a variety of platforms. LastPass provides a simple and efficient tool for higher education institutions that helps overburdened IT teams secure access to highly sensitive data and deploy cybersecurity initiatives campus wide.

For higher education institutions, LastPass provides password management for everyone on and off campus to protect personal passwords with a secure, private vault that's accessible from any device and browser. All LastPass business account holders receive Families as a Benefit—a premium personal LastPass account with six total licenses—to share with those closest to them. Individuals without a business account will receive a single premium LastPass account—perfect for a student population.

KIM MILFORD

Kim Milford serves as Executive Director of the Research & Education Networks Information Sharing & Analysis Center (REN-ISAC), which includes over 650 member institutions within the higher education and research community. REN-ISAC promotes cybersecurity operational protections and response.

LastPass •••|

Increase control and visibility with a password management solution that is easy to manage and effortless to use.

Learn More