Name: Code.org
Industry: Computer Science Non-Profit
Location: Seattle, Washington
Employees: 70 full-time

Challenge

- Growing number of tools increased number of shared passwords among the team
- Increasing staff turnover led to concern over password security

Solution

- Centralizing passwords in one secure system
- Provisioning and deprovisioning users in real-time, while maintaining control over departing employee passwords
- Syncing shared passwords among the appropriate team members

Non-Profit Code.org Goes High-Tech with Passwords

Challenge

Launched in 2013, Code.org® is a non-profit dedicated to expanding participation in computer science by making it available in more schools, and increasing participation by women and minorities. Code.org accomplishes their mission by designing curriculum, training teachers, partnering with school districts, and spreading awareness to ensure that more students learn computer science. Code.org increases diversity in computer science by making all of its resources available for free and online so students of all backgrounds can access learning anywhere — at their skill-level, in their schools, and in ways that inspire them to keep learning. In addition, they created "Hour of Code," an online platform that offers 1-hour game-like tutorials that make learning how to code fun, accessible, and easy for everyone.

As an expanding organization working nationwide to effect change, Code.org began to experience "growing pains". In addition to staff turnover, as the organization changed and expanded, so did the needs of the staff and the number of technology tools in use. While their home base is in Seattle, Washington, the team manages projects across the United States. The entire team needed quick, flexible access to numerous accounts and tools they use to organize teacher training workshops, service students, and grow the organization.

But more importantly, they needed to address the security concerns that were raised in regards to passwords. Code.org needed to ensure that as employees were leaving the organization or when short-term contractors were utilized on a project basis, they were not putting the organization at risk and that remaining staff still had access to necessary accounts and tools. Controlling the onboarding and offboarding process, as well as maintaining oversight of who had access to what passwords, became critical to Code.org's growth and success.

> *"LastPass helped us alleviate our growing pains by providing increased organizational security."*
>
> **Michelle Page,**
> VP of Finance & Administration, Code.org

These concerns motivated Code.org to seek out a password management solution, one that was not only cost-effective for a non-profit organization, but one that addressed their needs to efficiently provision and deprovision staff, and facilitate a higher level of control over shared passwords. These needs led Code.org to implement LastPass Enterprise, a centralized, cost-effective team password manager that saves user's passwords and then logs in on their behalf to any password-protected websites. Employees enjoy access to their accounts from every computer and mobile device, while management can ensure that employees only have access to the necessary passwords and don't put the organization at risk when they leave.

Solution

After deploying LastPass Enterprise, Code.org saw immediate benefits in the onboarding and offboarding process for employees. LastPass helped Code.org alleviate "growing pains" by providing increased collaboration among teams and heightened organizational security. When staff left the organization, passwords could be accounted for and were not lost or at risk of being compromised. Rather, admins maintained control over all company passwords and re-assigned them to the necessary team members, while departing employee accounts could be deactivated in real-time.

> *"With LastPass, passwords were not lost when staff left and passwords could be securely shared among staff members needing to access our many shared technology tools. Administrators could ensure access to technology was appropriate and controlled."*

Now, passwords can also be securely shared among staff members who need to access many shared technology tool accounts. When new employees join the team, they can be quickly provisioned with the shared accounts they need to start contributing to the organization. Passwords to shared tools can be given to team members without losing accountability. LastPass Enterprise's detailed reporting log allows administrators to tie specific events back to specific employees, even when the password is shared among many members of the team.

LastPass Enterprise's centralized admin features also allowed administrators to ensure access to technology was appropriate and controlled. Rather than sharing passwords via insecure methods, passwords are now encrypted and shared directly through LastPass and only given to the employees who need them, with the appropriate access restrictions in place. These sharing features have allowed Code.org to build a stronger culture of security without slowing down employees.

"One of the best features of LastPass for me is the increased security it provides. It makes it easy for us to manage users and the accounts that they have access to."

Code.org has particularly benefited from the Personal Linked Accounts feature. By linking a personal LastPass account to an Enterprise LastPass account, employees can enjoy secure access to all of their passwords throughout the workday, without having to switch between two accounts.

By implementing LastPass Enterprise, Code.org has addressed their concerns about password security within the organization. The onboarding and offboarding processes have been simplified, while ensuring that administrators maintain oversight of company passwords. Team members can easily share passwords to shared accounts and tools, allowing for increased productivity and collaboration.

Try LastPass Enterprise free today at LastPass.com/enterprise