LastPass •••|

Case Study: Crunchr

crunchr

“LastPass to us is basic hygiene, it’s like having a shower every day. It makes sure that you’re clean and secure in everything you do”.

Jan Joris *Vereijken*, Chief Technology Officer

Challenge

Based in Amsterdam, Crunchr supports organizations globally to gather meaningful insights into workforce operations. They aid businesses in curating a healthy working environment through equipping people analysts, human resource teams, and leadership with data that can predict trends and enable them to mitigate employee churn. Jan Joris *Vereijken*, Chief Technology Officer at Crunchr, joined the organization five years ago; however, his impact on their security infrastructure preceded him. When *Vereijken's* friend, Dirk Jonker, founder of Crunchr, mentioned setting up his own business, *Vereijken* advised him to immediately invest in a password manager. *Vereijken* understood the importance of a password manager after his personal Twitter account was compromised in 2012 due to reused passwords. From then on, he recognized the risks of recycled credentials and the challenges of generating secure passwords.

Vereijken adds: *"I realized that I needed different passwords for different sites as this was the main culprit when it came to my compromised Twitter accounts."* As he searched for an adequate tool to support him in his personal life, a friend recommended LastPass.

Recognizing the risks associated with weak password hygiene, *Vereijken* advised Jonker to invest in LastPass to ensure that Crunchr minimized data being compromised and key information being exposed or lost from the very start of its operations.

Solution

In 2014, Crunchr invested in LastPass. As their team has expanded they've continued to add licences to ensure they maintain a secure infrastructure.

The LastPass Password Generator is used significantly across the team as it enables Crunchr employees to create random and secure passwords. Administrators can make sure their team's passwords are at least 12 characters long and contain letters, numbers, and special characters. *Vereijken* notes: *"I've learned that it's vital to have a unique password for each account, it's become a rule for all employees across the business."* By creating unique passwords for each application, employees are able to remain vigilant against phishing attacks and mitigate their potential impact.

LastPass's ability to be utilized across multiple devices was another key driver for *Vereijken*. The Crunchr team operates in a hybrid format, with 60% of the organization working remotely. Moreover, they utilize a varied range of tech across the business and wanted a solution that could be accessed on Apple iOS as well as Microsoft Windows. *Vereijken* adds: *"The ability to be accessed across varied operating systems was important for me. I wanted to make it an easy deployment for the team and have the password vaults readily available to them at any time, from any location. LastPass remains accessible across multiple platforms without compromising their user experience, which made it perfect for us."*

"It's not a discussion point for us, maintaining password hygiene with LastPass is just something that we all have to do."

Results

Since their investment, LastPass has become a staple for Crunchr employees. With thirty policies enabled, from a minimum credential limit for master passwords, prohibited password reuse, and enforced multi-factor authentication, Crunchr ensured the team took considerable steps to improve their password hygiene. With only one current weak master password in the entire organization, it's evident that LastPass has positively impacted the team's password behaviour. Their average security score is now at 86% and password strength at 85%. *Vereijken* adds: *"I'm personally at 94% on my security score, some of my team members have surpassed me!"*

Crunchr uses over 60 different cloud-based solutions ranging from Hubspot, Bitbucket, and Google Workspace. As they streamline their processes, they're hoping to embed single sign-on to simplify accessibility. Employees use password sharing across teams through LastPass on a weekly basis to enable safe collaboration. With LastPass's Shared Folders feature, administrators can manage accounts and ensure leaving employees are unable to retain access. *Vereijken* notes: *"We had someone leave the finance team recently, the first thing I did was modify the credentials. If the team is following our guidelines and accessing the passwords through Shared Folders, they wouldn't even realize that any changes have been made."*

"I have over a thousand logins accumulated within my LastPass vault and I can proudly say they each have their own credentials."

Learn how Crunchr increased their password security using LastPass.

Get in Touch