DASHLANE

THE EMPLOYEE GUIDE TO

How Credential Managers Work

How Dashlane protects you, your credentials, and other sensitive information

Now that your organization is using Dashlane, you might be wondering how our credential manager keeps your information safe.

Can Dashlane see your data? What features should you take advantage of? And what if Dashlane gets hacked?

A credential manager protects your accounts by helping you store, manage, and share credentials and other information securely.

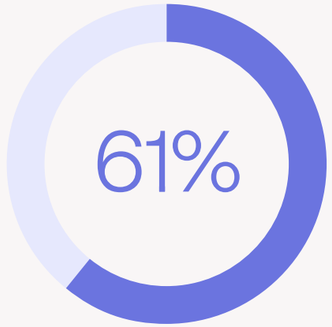
While countless digital tools aim to tighten cybersecurity, not all of them are equally secure. This guide explains why credential managers are the best tool for securing credentials, how credential managers work, how zero-knowledge architecture keeps your credentials secure, and how Dashlane's features protect your online activities and boost your organization's cybersecurity.

Why a secure, trustworthy credential manager makes a difference

$2.98 million

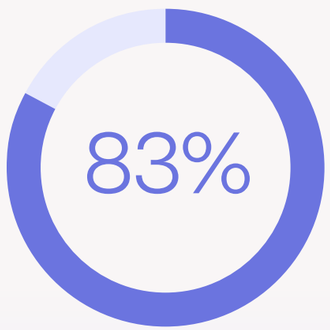
It can protect you from costly breaches

The average cost of a data breach for an organization with fewer than 500 employees is $2.98 million



It can reduce the chance of a data breach

61% of data breaches across all sectors involve compromised credentials



It can help you meet customer expectations

83% of consumers prefer to do business with companies that prioritize their data protection

It can increase employee adoption rates

Lack of trust is the second biggest reason employees use a credential manager (uncertainty about features is the main reason)

1. IBM Security, "Cost of a Data Breach Report," 2021.
2. Verizon, "2021 Data Breach Investigations Report," May 2021.
3. Shred-it, "Data Protection Report 2020," October 2020.
4. Dashlane, "The Future of Secure Work for People + Organizations," May 2022.

SECTION 1

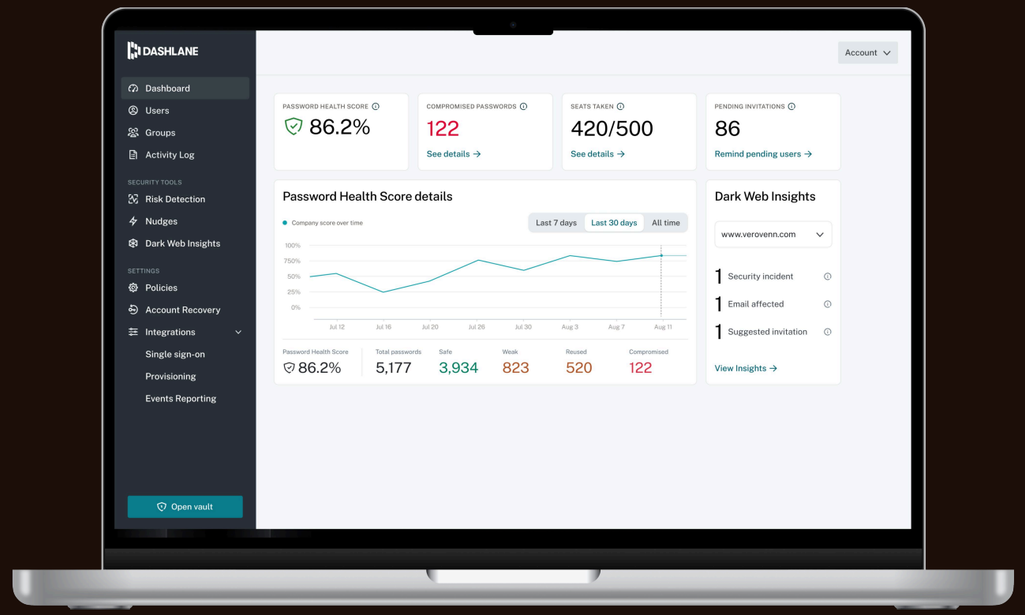
Credential management 101

Safeguarding your credentials is one of the simplest and most impactful ways for you to protect yourself and your workplace from hacks and breaches. When you use weak or compromised passwords, you're putting yourself and your organization at risk. Even your personal credentials can be an attack vector if you're reusing them at work, which is why it's important to be protected everywhere.

Passwords are highly valuable to cybercriminals. Stolen or weak passwords allow them to bypass cybersecurity measures such as firewalls and endpoint security because they can simply log in to accounts to access your company's information systems or data directly. Once inside, stealthy attackers can carry out their objectives without detection for a long time—often for weeks, months, and even years.

Recent major breaches started with one compromised password. For example, the supply chain attack on SolarWinds, which gave threat actors access to government and private company systems, was blamed on a weak password (solarwinds123) used by an intern. A compromised employee password also led to a major breach at GoDaddy, one of the largest website hosts, exposing the data of more than 1 million customers.

Following best practices, such as using unique, strong passwords and securely storing them, prevents your passwords from being compromised—and credential managers like Dashlane make this possible.



How a credential manager works

A credential manager is a software application that stores all your credentials in a secure location. The app creates long, random, unique passwords for you, and you don't have to memorize them or write them down.

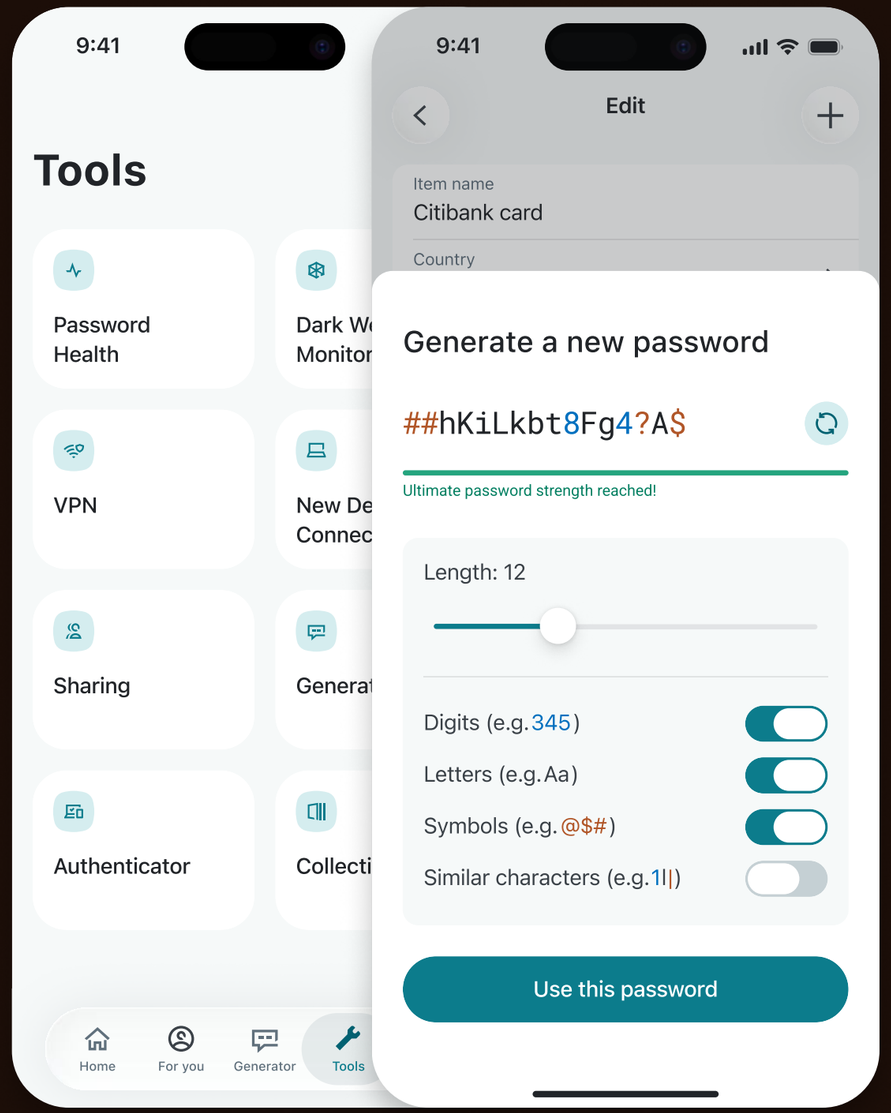
Unlike passwords stored through other means, such as spreadsheets, email, and browsers, credentials stored in a credential manager are encrypted—and, in the case of Dashlane, can only be decrypted on a verified device associated with you.

In addition to being secure, credential managers are convenient and simple for you to use because they:

- Sync across all your devices so you can access your accounts from your computer, laptop, tablet, and mobile device anytime
- Eliminate the need for you to memorize all passwords except the master one that unlocks your credential management app
- Allow you to quickly and safely share passwords with co-workers for shared accounts or for onboarding purposes

Credential managers allow you to easily follow best practices recommended by cybersecurity authorities such as the National Institute of Standards and Technology (NIST) and U.S. Cybersecurity and Infrastructure Security Agency (CISA)—without negatively impacting your productivity. **Here are examples of some recommended practices that are simple to adopt with a credential manager:**

- Use a different, strong password for each account
- Don't use personal information (including pet names and anything that can be guessed from social media) or dictionary words from any language to create passwords
- Use the longest password or passphrase that each account allows
- Require at least two methods of user identity authentication via 2-factor authentication (2FA) or multi-factor authentication (MFA) whenever possible
- Update passwords for any accounts that have been compromised in a data breach or another security incident
- Don’t write down passwords and leave them on your desk or taped to your computer
- Don’t store passwords in your web browser
- Use a credential manager to generate and store unique passwords



CASE STUDY:

How a compromised password brought down Colonial Pipeline

The 2021 Colonial Pipeline ransomware attack that crippled the largest U.S. fuel pipeline started with one compromised password. The attackers gained initial entry via a virtual private network (VPN) account, which gave them access to the company's network. They used an employee's compromised VPN credential, likely obtained from the dark web.

The attack shut down operations for several days, causing widespread gas shortages and panic-buying on the East Coast. Colonial also paid a $4.4 million ransom, which was later partially recovered.

SECTION 2

How Dashlane makes access at work simple with secure credential management

Dashlane makes security simple so that, regardless of your technical literacy, you can easily secure your passwords and other sensitive information. The app uses “zero-knowledge” architecture (which means that Dashlane cannot see what you store in your account) to securely store your credentials and other data.

Here’s how core Dashlane features keep you secure and productive:

Credential management: Whether it’s your personal account or an internal business tool, Dashlane will remember all your passwords—so you don’t have to. The passwords sync across all your authorized devices, which means you’ll never have to hunt for your logins. Dashlane can also generate complex, randomized passwords for you, then save them to the vault with one click.

Single sign-on (SSO): If your workplace uses SSO, your admins can connect the employee directory with Dashlane. This combination allows you to log in to multiple accounts with one set of credentials, so you don’t have to enter your Dashlane Master Password—and interrupt your workflow.

Password health score: Dashlane shows you which passwords are reused, weak, or compromised, along with your overall Password Health score. Dashlane helps you prioritize which passwords to change by showing you the ones that put you at highest risk. Your company’s admin can also track the company-wide rating to get a better understanding of your organization’s security posture.

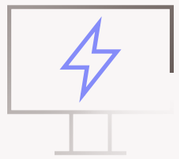
Secure information storage: In addition to passwords, keep your apartment access codes, your home’s Wi-Fi password, your login recovery keys, and other sensitive information safe and accessible to only you using Secure Notes. Dashlane even offers a dedicated space for IDs—where you can store passport numbers, government identification numbers, and other identification data—as well as a dedicated space for credit card information.

Secure sharing: Need to share sensitive information, like a password or a Secure Note? You can do that safely by simply choosing the credential or Secure Note you want to share, providing the person's or group's email address, and deciding whether you want to give that person or group full or partial rights to that credential or note. Dashlane will notify the recipient by email and in the app, then let you know when the sharing invite is accepted.

Autofill: When you visit a website after storing your information in Dashlane, the app autofills details such as your username, password, and payment information that you have stored. Autofill allows you to log in, fill out forms, and even pay for purchases with one click. The feature also protects you against phishing because the engine won't autofill credentials on malicious, lookalike phishing websites. The autofill engine relies on machine learning, which means it improves continuously.

Free family plan: Each Dashlane business user receives a free Dashlane Friends & Family plan to provide up to nine loved ones with the gift of a simpler, safer internet ($90 annual value). Use this plan as an opportunity to encourage good security habits for your loved ones.

Dark web monitoring: You can add up to five emails to be monitored on the dark web. When Dashlane finds passwords associated with those email addresses on the dark web, it flags them in the app and prompts you to change your password. Use the Password Generator feature to create a strong, random password as soon as possible to ensure a cybercriminal doesn't take advantage of the security compromise.



2FA: Add an extra layer of security to your online accounts by requiring a unique token or push authentication to verify your identity when you log in. For shared account credentials that have 2FA set up, the other person can also access the 2FA token.

Many organizations expect their employees to be proactive participants in cybersecurity and maintain good security habits. With Dashlane, you can do just that—without taking time away from your busy schedule.

SECTION 3

What makes Dashlane safe and secure?

Q&A

with Dashlane CTO Frédéric Rivain

How exactly does Dashlane protect my data?

Dashlane provides a secure, encryption-based cloud storage solution, built on what we call a zero-knowledge architecture. Our technical design ensures only the user, not Dashlane or any third party, can decrypt their vault. The platform combines device-level encryption and cloud secure enclaves to protect data at rest, in transit, and in use.

Having your data stored using zero-knowledge architecture is kind of like putting your data in a safe deposit box. You know what's in it. The bank knows the box exists and that you're likely storing something in it, but they don't know what it is.

"To be truly safe, you need to understand which technologies you can trust. I show people zero-knowledge encryption with Dashlane. I show them my digital wallet and don't worry about it because I know Dashlane keeps my information safe."

—Joe McLain, CIO at Buena Vista University

Check out more success stories →

Why is saving my passwords in my browser not a good idea?

Web browsers, such as Chrome and Safari, don't use zero-knowledge architecture to protect the information you store in them, which leaves you vulnerable in the event of a cyberattack. Hackers can steal and use your information however they see fit.

In addition, the companies that run the web browsers, such as Google for Chrome and Apple for Safari, can access the credentials saved in their browser if they want to. This means you're putting your trust in a big tech company to not access and use your data in a way you don't like. Dashlane, on the other hand, uses zero-knowledge architecture to protect all your information and, by extension, your privacy.

Can Dashlane see my data?

No, Dashlane can't see or access any user data whatsoever, including Master Passwords, because it doesn't store the information or have access to it in any way. This ensures your data remains just that—yours. Read more about our privacy policy here and our terms of service here.

If Dashlane gets hacked, do I get hacked?

No, a security incident affecting Dashlane wouldn't automatically expose your data. Your data is encrypted locally on your device before it's transmitted to our servers. The encryption keys are derived from information only you control, and Dashlane doesn't have access to them. Our zero-knowledge architecture is specifically designed to minimize risk and reduce the impact of a potential compromise.

How does Dark Web Monitoring work?

All you need to do is add up to five email addresses in the Dark Web Monitoring tool in Dashlane, and we'll track them for you to make sure they're not compromised on the dark web. We regularly scan the dark web for the email addresses you've added and any personal info related to them. If we find anything, you'll get a full report and will be prompted to change your passwords if any of your logins are compromised. Any time we find something concerning, you'll get an email alert from us and a pop-up the next time you open Dashlane.

The average internet user has 301 passwords. As you add more digital tools to your daily work routine, your risks of compromised credentials grow, and cybersecurity tools play an important role in minimizing those risks in both your personal and professional lives. Take the time to understand how trustworthy your cybersecurity tools are and how they keep you secure online—and get peace of mind whether you're at work or at home.

Learn how

Check out our other Resources on credential security, how Dashlane works, and more.

Visit our Resource Library →

Check out our Help Center →

Already using Dashlane? Learn the basics of Dashlane in a live webinar and Q&A session.

Sign up for admin webinar →

Sign up for employee webinar →

DASHLANE

About Dashlane

Dashlane provides complete credential security, protecting businesses against the threat of human risk. Our intelligent Omnix™ platform unifies credential protection and password management, equipping security teams with proactive intelligence, real-time response, and protected access to secure every employee. 25,000 brands worldwide, including leading enterprises such as Michelin, Air France, and Forrester, trust Dashlane for industry-leading innovations, patented zero-knowledge security, and an unmatched user experience.

Learn more at dashlane.com.

LinkedIn

Twitter

Instagram

Blog

Reddit