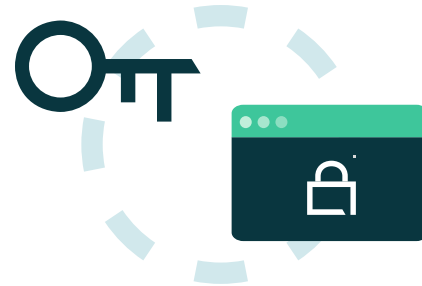




Password Management 101

Protecting your organization and your people with password best practices





Despite the digital technology evolution in the past couple of decades, passwords are often the only protective layer that stands between a malicious actor and your organization's data. Without strong password management practices in place, passwords represent one of the biggest threats to your cybersecurity.

Understanding three main topics can help you develop and implement secure password management across your organization:

- Industry developments that drive best practices
- The importance of password managers for maintaining these practices
- The role your people play in safeguarding access to your data

This e-book examines each of these elements and provides insights and tips on how to implement and maintain good password hygiene across your business.

Part 1

The Industry



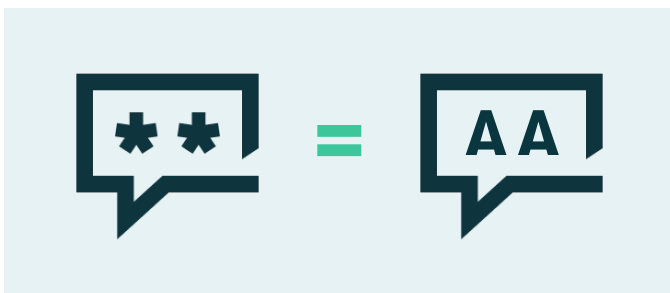
The evolution of passwords as a security tool



Decades ago, passwords were developed as a simple way to protect sensitive information, but this technique hasn't kept up with the pace of digital technology. Today, compromised passwords are the fastest and easiest way for someone to gain unauthorized access to your organization's data and systems.

And cybercriminals don't have to look very hard to find these proverbial keys to the kingdom.

The number of compromised credentials available on the dark web is astonishing and growing fast. Researchers found more than 6.7 billion unique credential pairs—combinations of usernames and passwords—on the dark web in 2022, a 34% increase from 2020.¹



Research shows that credentials are the main path that leads malicious actors into your organization. Last year, credentials were involved in about half of all data breaches that weren't the result of error or misuse—far ahead of other tactics like phishing and vulnerability exploitations.²

As the industry looks for ways to combat the password problem, a passwordless future is on the horizon. Passwordless authentication—which verifies user identity without requiring a password and uses an authenticator like a smartphone.

This promising development, however, is in its early stages, and wide adoption is years away. Passwords, in fact, may never completely disappear. In the meantime, implementing best practices for password management is critical for every business in the digital age. To make the transition seamless for your organization, any new authentication solution you implement should support both passwords and passkeys (passwordless authentication credentials).



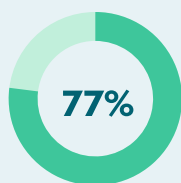
Evolving best practices for password management

Password management practices, too, have evolved through the years. Not that long ago, one common piece of advice was to change passwords regularly—as frequently as monthly or quarterly. Security experts have since learned that this policy only compels people to create easy-to-guess passwords and reuse passwords across accounts. Malicious actors count on both of these behaviors, using various tactics to crack weak passwords or leverage stolen credentials.

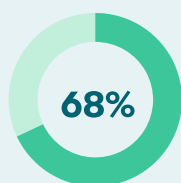
Current best practices include using a different strong password for each account, avoiding the use of personal information and dictionary words in passwords, and not sharing passwords through unsecured methods such as collaboration apps and email. (See page 9 for specific best practices.)

Requiring employees to follow these practices without a proper tool, however, doesn't lead to compliance. That's why security experts recommend adopting a password manager across your organization. This tool is designed to help your employees create, store, share, and manage passwords securely and conveniently.

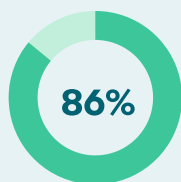
The state of today's threat landscape



of organizations report an increase in disruptive cyberattacks in the past 12 months, compared to only 59% the previous year³



increase in the number of data compromises in the U.S. in 2021⁴



of organizations experienced bulk phishing attacks in 2021, compared to 77% in 2020⁵

\$4.9 million

is the average cost of data breaches caused by phishing, which is the second most common cause of a breach⁶

#1 tactic

leading to data breaches is the use of stolen credentials⁷

3. EY, "Global Information Security Survey," 2021

4. Identity Theft Resource Center, "Data Breach Annual Report," 2021.

5. Proofpoint, "State of the Phish," 2022

6. IBM Security, "Cost of a Data Breach Report," 2022

7. Verizon, "Data Breach Investigations Report," 2022



Password managers as a compliance tool

Recently, there's been more emphasis from government entities, regulatory bodies, and industry groups on implementing a password policy and password management practices. One example is an [August 2022 circular from the U.S. Consumer Financial Protection Bureau \(CFPB\)](#), which stated that inadequate security of sensitive consumer data could violate prohibitions of unfair practices.

The bureau stated that cyberattacks could cause substantial harm to consumers and that failure to implement basic security practices significantly increases the likelihood of an unfair practices violation. One of the three best practices that CFPB recommended to avoid noncompliance is implementing password management policies and procedures.



Part 2

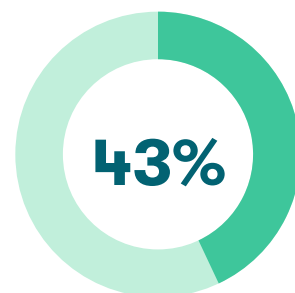
Password Managers



Implementing best practices with a password manager



With the proliferation of digital tools, employees are accessing a growing number of accounts, and each of those logins is a potential path to your sensitive data and systems. This risk is even greater with the rise in remote work because your employees are accessing their accounts from anywhere—including from unsecured devices and WiFi networks.



Only 43% of surveyed organizations feel prepared to respond to a data breach caused by a remote workforce⁸

How passwords put your organization at risk

Gaining access into your network by hacking into an employee account or using stolen credentials yields a much higher success rate for an attacker than trying to circumvent security tools such as a firewall. Consequently, exposed and weak passwords are one of the most common exploits used by cybercriminals.

Compromised and weak passwords expose your business to a number of risks, such as:

- Data breaches
- Ransomware attacks
- Identity fraud
- Account takeovers
- Financial fraud

Threat actors use compromised insider credentials at various stages of an attack to carry out actions such as:

- Gaining an initial foothold into your network or systems
- Escalating privileges and elevating access to critical accounts
- Deploying malware and ransomware
- Installing a backdoor into your systems



How a common attack unfolds

Cybersecurity professionals often use a seven-step model called the Cyber Kill Chain (first introduced by Lockheed Martin Corp.) to describe the stages of an attack. Note that not all attacks—for example, cloud attacks—follow this pattern, and some attacks don’t include all seven stages.

1 Reconnaissance

Threat actors establish the infrastructure (tools, tactics, etc.) needed for the attack. This may entail using a phishing kit, probing the target entity’s systems for vulnerabilities, finding high-value targets within the organization, collecting employee info from social networks, and gathering other intelligence about the organization. At this stage, they may also “shop” on the dark web for leaked corporate credentials.

2 Weaponization

The attackers create their attack vector and payload, such as malware to harvest credentials or an exploit for a vulnerability.

3 Delivery

The adversaries launch the attack, whether it’s by sending a phishing email with a malicious link to steal credentials, sending a malicious attachment with malware, hacking into a virtual private network, etc.

4 Exploitation

Once inside, the attackers look for further weaknesses to exploit. They may escalate privileges by gaining access to more logins, map the environment, and compromise new systems.

5 Installation

The attackers establish their control by installing more malware, remote access trojans, and backdoors.

6 Command and control (C2)

Establishing a C2 connection allows the attackers to control the system or identity remotely to deliver further instructions, expand access, and establish new access for future intrusions.

7 Actions

In this final stage, the intruders carry out their objectives. If their goal is to steal data, for example, they’ll begin collecting it on a staging server and then exfiltrate it.



Real-world cyberattacks involving compromised credentials

Uber (September 2022)

A hacker claiming to be 18 years old gained access to multiple critical Uber systems, including email, Slack, and source code. The attacker used a contractor's credentials, likely obtained on the dark web, along with social engineering to trick the person into approving a two-factor authentication (2FA) request. While the full impact of the attack will not be known for some time, Uber's reputation took a hit, especially since it's not the first time the company's systems have been compromised.

SolarWinds (December 2020)

A sophisticated supply chain attack that compromised the security of dozens of government and private sector organizations started with hackers gaining access to SolarWind's software code. The initial access point was attributed to an intern who used the password solarwinds123, which attackers likely obtained on the dark web. The attackers, who went undetected for months, inserted malicious code into one of SolarWinds' software updates, giving them access to high-profile companies and U.S. government agencies.

Twitter (July 2020)

A group of amateur hackers led by a 17-year-old mastermind used social engineering to trick Twitter employees into revealing their login credentials. They gained control of an internal support tool for the social media platform and commandeered more than 130 accounts, including those of high-profile elites and celebrities like Elon Musk, Barack Obama, Bill Gates, and Kanye West. The hackers tweeted a series of messages promoting a Bitcoin scheme, damaging Twitter's reputation.

“Our strongest tools are our reputation and relationships. A breach could do more than take our security; it could remove the trust from our name that we've worked so hard to build.”

**—Chelsea Richardson, Principal,
Vice President at JD+A**





Recommended best practices for password management



As we discussed earlier, your employees' poor password habits put your entire organization at risk. Here's why:

Reusing passwords: 63% of employees admit to recycling their passwords for multiple accounts⁹, and if one of those accounts is hacked, the credentials are likely to end up on the dark web. Attackers use those credentials to launch credential-stuffing attacks—relying on automated means to try cracking other accounts with the same logins.

Sharing passwords through unsecured channels: Many organizations share passwords via channels like Slack and email when onboarding new employees or sharing accounts. Since those channels are not encrypted, that data can be intercepted by a third party.

Storing passwords in a browser: Most people stay logged into their browser profile, which means others using the device could easily access their passwords. Additionally, passwords stored in the browser aren't encrypted and can be accessed remotely with the help of malware. The passwords are also at risk if the employee's device is lost or stolen.

Using weak or easy-to-guess passwords: One way hackers try to crack accounts is by using large lists of common passwords—anything from the all-time favorites “password” and “123456” to pop culture words—in what's called a credential-stuffing attack.

The top most common passwords in the U.S. [Read more](#) in our blog

Password	123456	123456789	12345	1234567890
Password1	1234567	12345678	1234	Qwerty123



With these risky habits in mind, here are the current recommended best practices for managing passwords:

- Use a different, unique, 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 provider allows
- Require at least two methods of user identity authentication through 2FA or 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

A password manager makes it simple to follow these best practices by doing most of the work for your employees—they don't have to come up with secure passwords or memorize them. The password manager also adds convenience by autofilling logins and offering a secure method for admins to share passwords across your business.

[Learn how](#) Dashlane can help your employees follow password best practices, and start a trial on us.

Password managers deemed a critical application

Following the massive outfall from the SolarWinds breach and other supply chain attacks, the U.S. president issued an order in 2021 to improve the nation's cybersecurity, with a special emphasis on the software supply chain. As part of the order, the National Institute of Standards and Technology (NIST), which sets cybersecurity standards for the U.S. government, included password managers on its list of software that's considered critical to the IT environment. While this order applies specifically to software developers that provide solutions to the government, this classification validates that password managers are essential to IT security.



Implementing a password manager for your business

Despite steadily rising risks and costs associated with password-related security incidents, justifying the time and costs of implementing a password management solution may still be a struggle. Part of it stems from the difficulty of quantifying the value of security tools when you can't accurately predict the likelihood, extent, or cost of a data breach for your organization.

One way to think about this dilemma is by comparing the potential costs of a security breach with the cost of implementing and maintaining your password management solution. Password managers are an inexpensive tool, whereas the average data breach cost is \$4.3 million globally.¹⁰



Business benefits of a password manager:

- Generates strong passwords that don't need to be memorized
- Enables people to securely share passwords
- Saves IT admins time and resources on onboarding and offboarding as well as managing logins
- Provides early alerts to data breaches and leaks on the dark web
- Tracks password health individually and company-wide
- Makes enforcing password policies easy

In addition to providing the most secure and convenient method for managing passwords, many password managers bring additional value through robust security features such as dark web monitoring and password health monitoring. They also offer simple tools for admins to help improve your organization's security posture and boost your security culture.



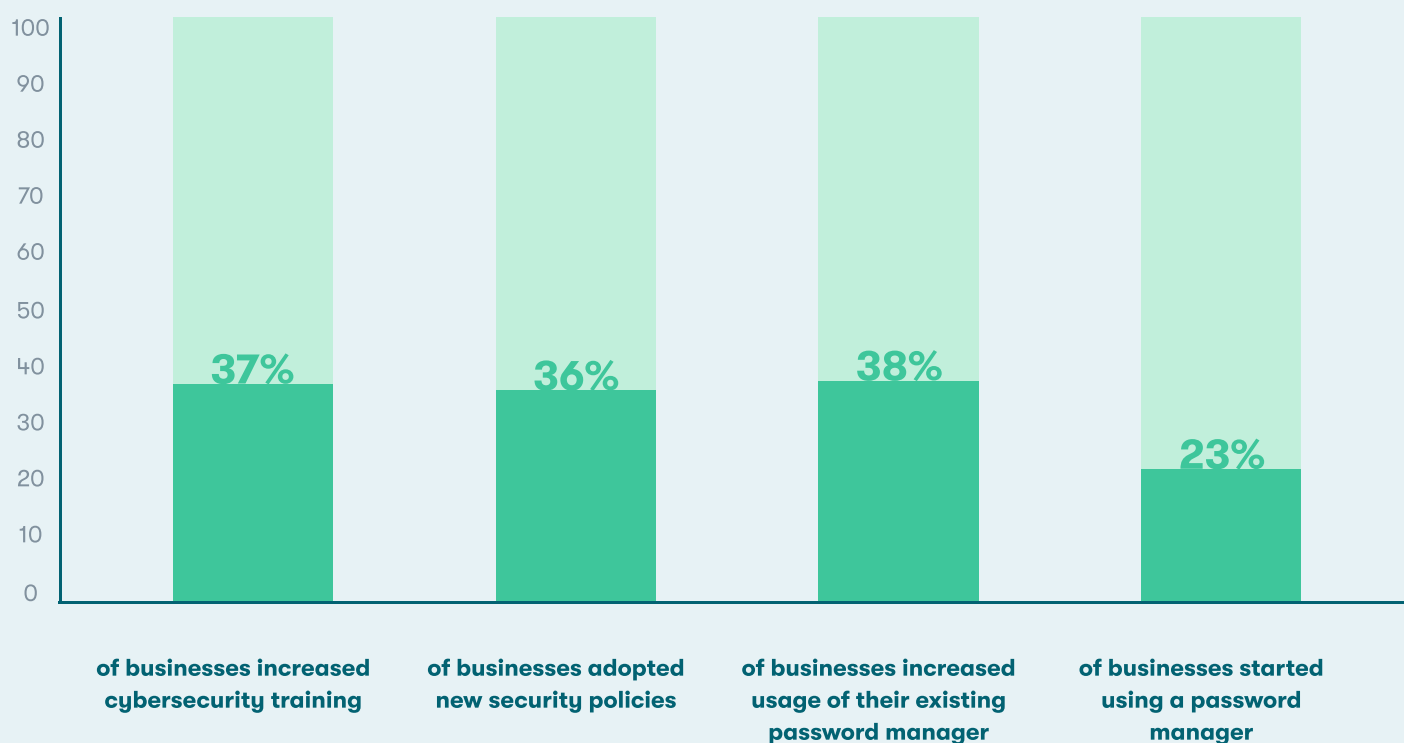
How a password manager works

A password 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 password manager are encrypted. Additionally, some password managers use what's called zero-knowledge architecture, which means the data you store on them can only be decrypted on a verified device associated with you. This provides an additional layer of security because no one else—whether it's malicious actors or the app vendor's employees—can view your passwords and other data.

Learn how Dashlane protects your data with zero-knowledge architecture and other features by downloading our e-book, ["The Employee Guide to How Password Managers Work."](#)

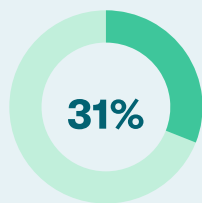
Cybersecurity awareness has increased year over year— but we still have a long way to go



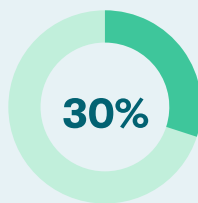


Overcoming adoption barriers

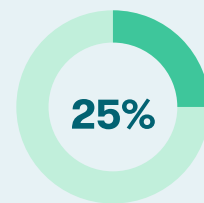
Just because you invest in cybersecurity tools doesn't mean your employees will actually use them. A recent Dashlane survey found three main roadblocks to password manager adoption:



of employees lack an understanding of the tool's features



lack trust in the vendor



have difficulty setting up the tool

If employees don't trust the tool or understand how it works, they simply won't use it. It's important to educate them about why they need a password manager, as well as what features are relevant to them and how those features improve security. In addition to providing ongoing awareness, incorporate password security education into your onboarding process, which will set up your employees for success from their first day on the job.

Disruptive implementation that impacts the entire organization is likely to cause resistance among employees and business leaders alike. No one wants to be locked out of their accounts while you're rolling out new login procedures. One way to overcome this hurdle is by choosing a solution that's simple to deploy across the organization and offers admin tools for easy onboarding and offboarding.

About half (52%) of employees believe their organization needs a password manager; among leaders, a resounding 97% feel the same. Yet only 41% of organizations require a password manager.¹¹



Features and capabilities to consider in a password manager

2FA: Built-in 2FA allows you to enable 2FA for your password manager through a third-party authenticator app, adding another layer of security for passwords and ensuring your authenticator token is always handy.

Autofill: By automatically filling in usernames, passwords, and 2FA codes on every account, autofill simplifies logins and allows employees to log into their online accounts with one or two clicks. This feature also adds additional security because it won't autofill credentials on lookalike accounts or phishing websites, and you can train employees to identify that as a red flag.

Password health management: As you add new accounts and digital tools, each reused, weak, or compromised password puts your organization at risk. A password health feature highlights those risky passwords for employees so they can change them as soon as possible.

Password sharing: The ability to create groups based on departments or other needs allows admins and individual employees to share passwords securely and efficiently.

Dark web insights and monitoring: By scanning billions of records on the dark web for any leaked data and alerting employees when their information is involved in data leaks, a dark web insights feature enables employees to quickly remediate password threats. Additionally, some solutions provide a dark web monitoring dashboard for IT admins so they can access real-time insights and alerts about security breaches and other vulnerabilities facing employees.





Features and capabilities to consider in a password manager



Onboarding/offboarding: Complex rollout and onboarding create hurdles for adopting new tools, and simplifying processes such as policy setup and provisioning helps overcome those barriers.

SAML-based single sign-on (SSO): SSO support that's built into your password manager helps you integrate your tool with your identity provider (e.g., Azure AD, Google Workspace, JumpCloud, etc.) so employees can use their SSO credentials instead of their master password to access their password manager.

Tracking and measuring: A solution that gives your admins visibility into company-wide password security posture and measures improvements over time is an invaluable tool that helps you identify risks and take steps to mitigate them.

Separation of business and personal spaces: Some solutions allow employees to separate their personal and business passwords, which simplifies offboarding when they leave your business. Employees automatically lose access to corporate credentials while retaining access to their personal ones, providing peace of mind that they'll always have access to their personal data stored in the password manager.

[Sign up for a free trial](#) of Dashlane Business to learn how Dashlane can help your business boost security and productivity.

Part 3

Your People



Successful password manager adoption with human-centric policies

People are the most important part of maintaining password management best practices. And employees want to do their part to protect your business—79% of participants in a [Harris Poll](#) said they take some personal responsibility for their company's overall security. But, as we touched on earlier, simply providing the right tools will not lead to improved cybersecurity.

Successful implementation relies on a strong security culture. [A human-centric security culture](#) empowers employees to actively participate in defending your business and adopt secure password management habits. Use employee training and awareness in tandem with your password manager's security features to improve the effectiveness of your efforts.

Secure password management is most likely to flourish in a corporate culture that prioritizes employee engagement and a proactive commitment to security. That's why it's critical to foster a sense of ownership and pride in participation. Employees must fully grasp the real-world consequences of poor cybersecurity hygiene, which can potentially entail millions of dollars in financial losses. Each employee, regardless of job title, must also know their singular role and responsibilities in the collective effort to protect data assets, applications, and networks.

Steps to improving security culture include:

- **Raising employee awareness:** Help employees understand how their behavior impacts your company's data privacy and security. Educate them about the best practices that help protect them and the business.
- **Tracking progress over time:** Measure your security training effectiveness by using admin tools such as organization-wide password health tracking. Some password management solutions also enable admins to identify risky employees by monitoring who is not taking actions to improve their password health.
- **Reiterate based on results:** Revise your tactics based on progress. This may include sending email reminders to employees about good password habits, strengthening your password policies, or creating new awareness programs.



When you get ready to roll out your password management policies and tools, your security culture can serve as a launching pad. Build on your current awareness efforts to talk about the importance of maintaining best practices for passwords. But don't stop there. To get employee buy-in, your pre-rollout communication campaign should also explain how the password manager's features make security simple for employees while boosting both their productivity and security.

If you have a hybrid environment, don't forget to engage remote employees and make the transition as smooth for them as you do for your in-office team. That's where a password manager with strong onboarding and offboarding capabilities is especially important. Additionally, provide ample online training opportunities and take advantage of all the educational resources that your vendor offers.



Pro tip:

Create and communicate your new password policies before rollout

Before you deploy the solution across your organization, create password policies that will help employees understand the new procedures, requirements, and expectations. The policy document can be very simple—even shorter than a page—but should cover key requirements for password management, such as:

- The approved password management solution
- The acceptable security score for user credentials
- Basic best practices for sharing and storing passwords

Avoid including jargon, fear-mongering, and vague language in your policy. Focus on emphasizing how strong passwords protect employees and your business, explain key concepts to ensure everyone understands the terminology, and use precise language when describing expectations and requirements.

[Read our blog](#) to learn more about creating employee-friendly password policies.



Resources for successful implementation

Use Dashlane's [resource library](#) and blog to help employees learn about password management and to get practical advice and tips for admins. Below is a quick list of helpful resources.

For employees:

- **E-book:** [Essential Guide to Common Cybersecurity Terms](#)
- **Slide deck:** [Why Improving Password Management Matters](#)
- **E-book:** [The Employee Guide to How Password Managers Work](#)
- **Blog:** [Best Ways to Store Passwords at Home or Work](#)
- **Blog:** [A Beginner's Guide to Two-Factor Authentication](#)
- **Blog:** [How Strong Is Your Password and Should You Change It?](#)

For admins:

- **Blog:** [How Admins Can Simplify Provisioning](#)
- **E-book:** [Identity and Access Management 101](#)
- **E-book:** [Definitive Guide to Password Management for Small Businesses](#)
- **Webinar:** [The People vs. Policy: Building a Human-Centric Security Culture](#)
- **Blog:** [Creating a Password Policy Employees Will Actually Follow](#)
- **Blog:** [How to Manage Passwords at a Business Level](#)


What's Next

Passwords will remain ubiquitous for the foreseeable future, and safeguarding them is mission-critical for your business. A password manager is an effective and low-cost tool to do just that—protect your organization's people, data, and other assets.

Learn more about securing your corporate passwords, improving policies, and kickstarting your security culture. **Download our e-book, "A Practical Guide to Cybersecurity with a Password Manager."**

About Dashlane

Dashlane is an advanced password manager for businesses that is as easy to use as it is secure. The award-winning solution fuses the security capabilities of IAM and password management to simplify and streamline data protection. Dashlane is built on a patented security architecture that integrates 2-factor authentication, single sign-on, and AES 256-bit encryption with powerful password management capabilities. Dashlane has empowered over 15 million users and over 20,000 companies in 180 countries to enjoy a simpler, more secure internet.

-  [LinkedIn](#)
-  [Twitter](#)
-  [Instagram](#)
-  [Reddit](#)
-  [Blog](#)

[Dashlane.com](https://dashlane.com)

