Password Playbook for Small Businesses

How to create, manage, and share passwords easily and securely

DASHLANE

Table of contents

As your business grows, so do you and your team's responsibilities. One important area that will continue to demand your attention? Protecting your company and data from cybersecurity threats.

Data breaches and leaks are now a concern for all companies, regardless of size. But small businesses have the added challenge of limited staff and resources that can be dedicated to cybersecurity tasks—and you're already wearing more than enough hats.

The good news? A password manager helps you safeguard sensitive information and protect your business—and brand reputation—while boosting employee productivity.

In this playbook, we show you how small-business leaders can manage passwords to secure company and employee accounts and protect sensitive data—all while improving productivity.

Small businesses are embracing the opportunities that modern technology like the cloud gives them—but they're also starting to realize this technology creates security risks.

In response to the pandemic, 72% of surveyed small businesses (with 50–499 employees) across the world said they have accelerated their digital transformation projects.[1] Such rapid adoption of technology has left many small businesses vulnerable to cybersecurity threats. Common threats include:

- **Compromised passwords:** Nearly a third of cybersecurity incidents at small businesses resulted in data breaches in 2020, and login credentials became compromised in 44% of the confirmed breaches.[2]
- **Social engineering and phishing-related attacks:** Social engineering remains the top culprit behind data breaches for businesses of all sizes, and phishing is the top type of action involved.[2]
- **Ransomware:** Nearly 80% of managed security providers (MSPs) surveyed in 2020 reported that their small- and medium-business customers experienced a ransomware attack in the last two years, and 92% predicted that these attacks will get worse.[3]

You work hard to grow your business and serve your customers. You can't afford a data breach, which could result not only in devastating financial costs but also in loss of customers and business opportunities. To protect your growing company, you need the tools to secure your data access and accounts.

Costs of cybersecurity incidents to small businesses

Median costs of incidents and breaches to small businesses in 2020:*

No. of employees	Cost
1–9	$7,000
10–49	$17,000
50–249	$50,000
250–000	$133,000

*Based on data from eight countries
Source: Hiscox, "Hiscox Cyber Readiness Report," 2020

[1] IDC/Cisco, "2020 Small Business Digital Transformation," 2020
[2] Verizon, "2021 Data Breach Investigations Report," May 2021
[3] Datto, "Datto's Global State of the Channel Ransomware Report," 2020

How vulnerable are small businesses?

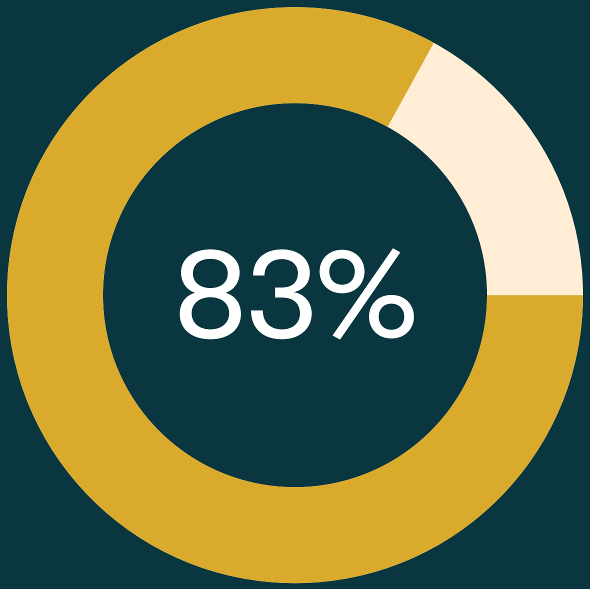
Cybersecurity is the top challenge when it comes to implementing technology solutions for small and medium companies.[1] Despite security concerns, however, many small businesses are not taking the right steps to protect themselves.

Among companies with 50 or fewer employees, for example, 43% of business leaders don't have a cybersecurity defense plan.[2] And while 65% manage their cybersecurity in-house, fewer than 10% of those businesses have an employee dedicated to IT. Cybercriminals know that small businesses don't have the staff and resources to devote to cybersecurity—and that's why they see small businesses as easy targets for attacks.

Unfortunately, your business becomes more vulnerable as you adopt more digital tools and apps. When your employees are accessing a variety of accounts from anywhere or reusing their passwords, they're creating a bigger attack surface for threat actors.

That's why a tool like a password manager is more important than ever, helping you address the growing risks of your digital business.

1. SMB Group, "SMB Digital Transformation Trends," June 2021
2. BullGuard, "New Study Reveals One In Three SMBs Use Free Consumer Cybersecurity And One In Five Use No Endpoint Security At All," February 2020



Food for thought

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

Source: Shred-it, "Data Protection Report 2020," October 2020

Storing passwords outside of a password manager is not only risky but can be incredibly ineffective, both for admins and employees. Many admins resort to things like spreadsheets to keep track of logins. But the manual process of managing even a small team's credentials quickly becomes cumbersome and time-consuming.

In the typical small business, IT duties like managing passwords often fall to the owner, general manager, webmaster, or some other employee who has various other day-to-day responsibilities. And if there's an IT admin, that employee is already stretched thin, wearing many hats from help desk and network management to email administration and cybersecurity. Employee password resets and other password management tasks place an unnecessary burden on whoever fulfills the admin role.

Consider some of the tasks involved for admins:

1. Onboarding and offboarding team members
2. Tracking down passwords for shared accounts
3. Resetting passwords manually when someone forgets their login
4. Getting the 2FA code if someone is OOO
5. Recovering 2FA rights for an account managed by a former employee

When you add in multiple accounts and cloud-based services for each employee, the time spent on these tasks quickly adds up. In an expanding business that continues to adopt new digital tools, manual practices for managing account access become simply unsustainable.

For individual employees, keeping track of passwords can also be frustrating, as can the time spent typing in credentials whenever they need to access a cloud service. That's why many resort to shortcuts like storing passwords in web browsers, compromising the security of your accounts and data.

Are passwords impacting your productivity? You're not alone.

In a 2021 survey of 1,000 employees, Dashlane found that:

- **35%** of respondents feel overwhelmed by keeping track of all their account information and logins
- **18%** feel they're wasting a lot of time trying to get into online accounts
- **49%** create their own tricks and shortcuts for managing logins
- **69%** retrieve or reset their passwords at least monthly

Source: Dashlane, "The Future of Security in the Hybrid Workforce," 2021

Data breaches that make the biggest headlines often involve large companies or massive numbers of impacted consumers. But small businesses suffer cyberattacks and data breaches just as regularly as big enterprises. Although those incidents often fly under the public radar, there are still plenty of examples of how small businesses get hit.

And, of course, there's no shortage of headlines about cyberattacks and data leaks involving cloud services and apps that small businesses use. When these providers experience a data breach, their user account credentials are typically sold or leaked on the dark web. Cybercriminals count on the fact that many of those users recycle their logins for other websites and services, and the attackers use these compromised credentials to gain access to other systems and services.

These three incidents illustrate some of the password-related risks and implications for small businesses.

Imperium Health phishing attack

Imperium Health Management, a small Kentucky company that provides development services to Accountable Care Organizations (ACO), experienced a data breach in September 2020 that affected nearly 140,000 individuals. The incident began with employees clicking on phishing emails, which included links to websites that harvested their email login credentials. The compromised email accounts contained customers' personally identifiable information (PII) and protected health information (PHI).[1]

Listen in to this conversation and Q&A with white hat hacker Rachel Tobac on demystifying the fundamentals of cybersecurity for you and your business.

[1] HIPAA Journal, "PHI of Almost 140,000 Individuals Potentially Compromised in Imperium Health Phishing Attack," September 2020

3 | Real-world examples (con.)

The stolen A-list celebrity data

Grubman Shire Meiselas & Sacks, a small but prominent legal firm for the entertainment industry, came into the spotlight in 2020 after cyberattackers stole 756 gigabytes of PII and other sensitive data on the law firm's high-profile clients (which include Hollywood A-listers, top athletes, and famous performers). The cybercriminals initially requested a $21 million ransom but doubled it when the company didn't cooperate. They also leaked a 2.4-gigabyte folder containing Lady Gaga's legal documents.[1]

The cybercriminals used REvil ransomware, which is commonly deployed in so-called double-extortion schemes that both demand payment to restore access and threaten to publish sensitive data for nonpayment. REvil often uses a phishing email or compromised credentials for Remote Desktop Protocol (RDP) as the initial attack vector.[2]

The Facebook data breach

A couple of years ago, Facebook had a massive breach that exposed some 600 million passwords (stored in plain text for more than seven years!).[3] Surveys show that 63% of people reuse passwords.[4] So chances are high that some of your employees reuse their personal login credentials for corporate accounts. By doing so, they're making a cybercriminal's job ridiculously easy.

And keep in mind this was not the first time Facebook has had a security incident, and the problem is not unique to Facebook. Other popular services that had user credentials compromised include LinkedIn, YouTube, TikTok, Zoom, and Dropbox, among others. Do you know how many of those compromised passwords are still circulating in your company, granting access to a lot more than just cloud apps and online services?

Want to learn more about steps you and your team can take to prevent data breaches and hacks? Download "A Business Guide to Data Breaches and Hacks."

1. Threatpost, "REvil Ransomware Attack Hits A-List Celeb Law Firm," May 2020
2. CSO, "REvil ransomware explained: A widespread extortion operation," November 2020
3. Forbes, "Facebook's Password Breach Suggests The Public Sees Cybersecurity As Obsolete," March 2019
4. Visual Objects, Worker cybersecurity survey, November 2020

Now that you understand the risks that small businesses face, let's get started securing important accounts (and protecting your customer data).

First, take a look at the accounts your team needs.

The more accounts, the higher your security risk if you're not using password management best practices. Shared logins, reused credentials, failure to change passwords regularly, and the lack of 2FA are among the factors that increase your security risks.

Here are some common accounts used by small businesses:

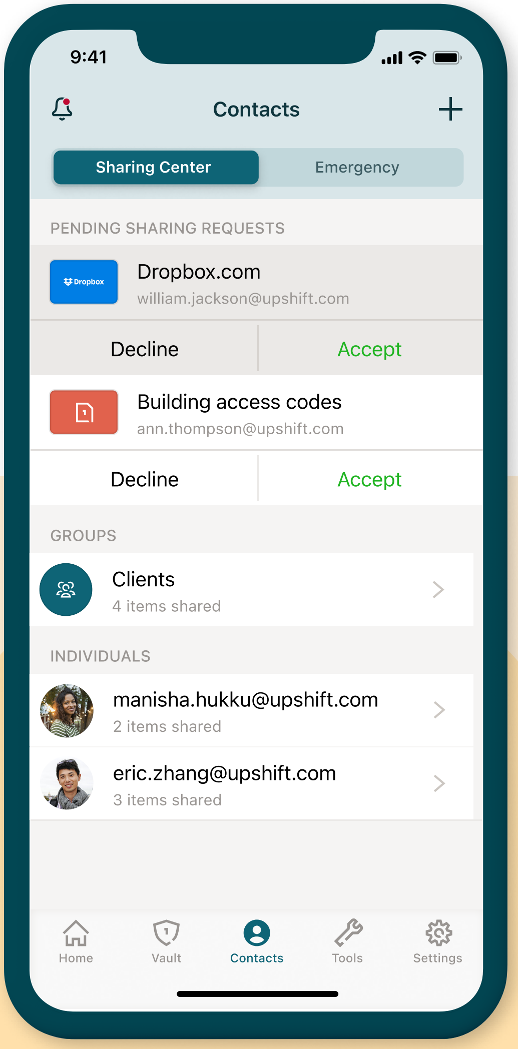
- MailChimp
- Zoom
- Microsoft 365
- Facebook
- Instagram
- Asana
- Monday.com
- HubSpot
- Salesforce
- Slack
- FreshBooks
- Xero
- Gmail
- Calendly
- Dropbox
- Google Suite

Use the checklist below as a starting point to understand your logins ecosystem.

Account	Owner?	Is this login shared?	How is it shared?	Is 2FA set up?	Is this password used for other accounts?
HubSpot	Otto Loggins	Yes	Spreadsheet	No	Yes

Now that you have an understanding of your most important accounts (and how those are being shared), head to the next section for how to secure them.

You pack a lot of tasks into your daily schedule. Your priority is on running and growing your business, not on figuring out how to use new apps. You need tools that are simple and convenient and don't hinder your ability to collaborate and communicate with employees and customers—whether you're on site, at your home office, or on the go.



9:41

Contacts

Sharing Center | Emergency

PENDING SHARING REQUESTS

Dropbox.com
william.jackson@upshift.com
Decline | Accept

Building access codes
ann.thompson@upshift.com
Decline | Accept

GROUPS

Clients
4 items shared

INDIVIDUALS

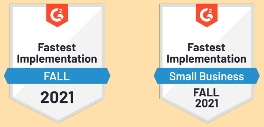
manisha.hukku@upshift.com
2 items shared

eric.zhang@upshift.com
3 items shared

Dashlane makes password management easy by:

- Filling in all your passwords across the web, on any device
- Saving logins as employees browse the internet
- Autofilling usernames, passwords, and 2FA codes on every account
- Enabling secure sharing of passwords and 2FA codes (e.g., for shared social accounts or for onboarding purposes)

And you can rest assured that your data is always secure. We use the strongest encryption available and zero-knowledge security architecture, so the info stored in each account is only accessible to the individual user. Plus, two-factor authentication is built right in.



Haven't started using Dashlane yet?
Sign up for a free trial today.

Here's how to get started. →

Onboarding (and offboarding) made easy

Complicated rollout and onboarding processes can hinder adoption of tools like password managers, especially for a growing business. As your security practices mature and you adopt new tools like single sign-on (SSO), Dashlane helps admins simplify onboarding. In addition to support for SSO, we offer video tutorials, guides, and templates to help you with successful adoption and onboarding.

Want to see how easy it is to get started? Check out our onboarding video series.

Set up groups

The Group Sharing feature allows Dashlane users to easily and efficiently share passwords and Secure Notes, making onboarding easy and secure. Admins can create groups based on departments or company needs in the Admin Console. Once created, both admins and individual users can share information with these groups via the app. With Dashlane, say hello to secure sharing and goodbye to Slacking or emailing passwords.

Now that you've got the basics down, let's talk about what's next and some of Dashlane's more advanced features.

Set up Dark Web Monitoring

Dashlane monitors the dark web for compromised credentials. When Dashlane finds an employee's username and password on the dark web, those credentials are immediately flagged in the app. The app prompts the employee to change the password—and provides a password generator for creating a strong, random password. Employees can add up to five email addresses to be monitored.

With these tools and tactics at your disposal, you can make your employees more secure—and productive—in no time.

Monitor and measure

Every user gets a Password Health Score that shows a breakdown of weak, reused, or compromised passwords. In the Admin Console, you'll be able to access your reporting dashboard. The dashboard's centralized view gives you unprecedented visibility into your company's password security and the ability to track improvements over time. There, you'll receive actionable insights on your employees' Password Health Scores and be able to help at-risk employees update their weak, reused, or compromised passwords. As more employees update their passwords, you can track score improvement over time.

Build a culture of security

Keeping your company data and reputation protected is not simply about the tools and processes you use—it starts with your employees. Dashlane enables admins to make employees part of the security conversation and educate them about their active role in protecting your organization.

With Dashlane, admins can:

- Track the overall company Password Health over time
- Benchmark security scores and measure progress
- Identify risky employees and engage them in discussions about safe password practices

See how Dashlane can help your small business.

Reach out or start a trial today.

You and your team are instrumental to protecting your business and maintaining customer trust and brand reputation. But you're experts in your products and services, not in cybersecurity. Ensure you and your employees can focus on keeping customers happy—instead of worrying about having your credentials compromised.

Follow us on:

DASHLANE