PASSWORD MANAGERS

Your Ultimate Guide

DOVE TECHNOLOGIES

TABLE OF CONENTS

PASSWORDS.

A NECESSARY EVIL HATED BY EVERYONE.

THEY'RE EITHER TOO HARD TO REMEMBER
OR TOO EASY TO GUESS.

IS THERE A SECURE ALTERNATIVE?

DOVE TECHNOLOGIES

This is what causes people to have poor password hygiene. Password hygiene refers to the degree to which a user's passwords are selected and managed according to best practices.

Poor password hygiene such as relying on weak passwords or reusing them across several logins is bad. We all know that.

But it's likely that someone, somewhere in your business is relying on a weak or reused password to protect their access to a critical system.

DOVE TECHNOLOGIES

IT'S A RISKY BUSINESS DECISION

Over 80% of hacking Related breaches were related to password issues in 2019.

SRC: 2019 VERIZON DATA BREACH INVESTIGATIONS REPORT

DOVE TECHNOLOGIES

A password manager will create and save unique, complex passwords for each site you use. When you login, it will automatically fill in the login boxes for you. These applications work on your computer and phone.

A password manager is simple and easy. Once it's set up, you only need to remember your master password.

Some examples of password managers are LastPass, Dashlane, and Keeper. We'll explain in depth which manager is best for you later in the book. For now, let's look at the benefits of a password manager.

What are the benefits of using a password manager?

- Autogenerates unique, complex passwords which are virtually impossible to guess

- A good password manager will sync across operating systems and browsers. That means if you use Windows for work, but have an iPhone, it's no worry.

It can help to protect your identity. By using unique passwords across every account, you segment your data. If one account is breached, it's highly unlikely others will be.

DOVE TECHNOLOGIES

What are the benefits of using a password manager?

- It can alert you to risk. If you land on a fake website your password manager won't autofill your data because it won't recognize the site as being valid.

- Some password managers scan the dark web to make sure your credentials haven't been leaked

- Many password managers operate a zero-knowledge approach, which means your data is encrypted before it leaves your device.

DOVE TECHNOLOGIES

BUT, LIKE ALL GOOD THINGS, THERE ARE DRAWBACKS.

DOVE TECHNOLOGIES

What are the risks of using a password manager?

- All your sensitive data is in one place, protected by one master password.

- It's possible cyber criminals could get hold of your master password, for example if you had malware or a keyboard logger watching what you do.

- You definitely need to use biometrics or multi-factor authentication (MFA, where you use a separate device) to prove it's you.

- If you forget your master password, it's deliberately difficult to reset it

DOVE TECHNOLOGIES

Now that you know the benefits and risks of password managers in general, it's time to learn the three (3) main types of managers available and their pros and cons.

The main types are:

Browser Based

Cloud Based

Desktop Based

DOVE TECHNOLOGIES

Browser Based

This is the password manager that's built into your browser such as Chrome, Edge, and Safari. Browser-based password managers are free and easy to use, but that's where the benefits end.

They're not a solution we'd recommend, especially for a business. They only work within their own browser, so if you wish to change to another, you either have to export your data or start over. They are limited in their use over multiple devices.

DOVE TECHNOLOGIES

Cloud Based

These password managers store everything in the cloud. They're safer than browser-based alternatives as they come with features to enhance security.

Firstly, they provide a backup of your vault, meaning your data isn't lost if your device is. Cloud-based password managers also let you store other sensitive data, like credit card details and secure notes, giving an additional level of data protection.

They can detect weak and reused passwords and generate new stronger ones.

DOVE TECHNOLOGIES

Cloud Based

Some will even run checks to make sure your data hasn't leaked. You're also able to share secure data easily, with co-workers or family for instance, even if

And cloud-based password managers have the benefit of working across multiple browsers, operating systems, and mobile devices. You don't have to think about anything – your password manager just works.

DOVE TECHNOLOGIES

Desktop Based

Desktop-based password managers can be the safest type, but that all depends on how security conscious you and your team are.

Just because something is the safest option, doesn't necessarily mean it's the best option for your business.

These store data locally on one of your devices. And that device doesn't have to be connected to the internet. That's a benefit because it means the chances of it being breached are lower.

DOVE TECHNOLOGIES

Desktop Based

If you use a biometric login for your master password you'll be even safer from rare-but-risky keyboard logger attacks (this is where malicious software secretly records everything you type into your computer).

The downside to desktop-based password managers is that you'll need to make sure you take your own regular backups of your data and vault. Otherwise, if your device breaks beyond repair or is stolen, your vault is gone. Another issue is that you can't access your passwords from other devices, and sharing can be difficult too.

DOVE TECHNOLOGIES

ARE PASSWORD MANAGERS SAFE?

DOVE TECHNOLOGIES

The answer is...
YES.

Although there have been breaches in the past, most professional password managers have an outstanding record.

If you and your team always follow password manager best practice – more on this later – you'll be highly protected from credential theft.

Premium paid-for services offer a lot more protection, too. There are more features you can take advantage of for better usability, additional security, and safe sharing... all of which are really important for business use.

DOVE TECHNOLOGIES

PASSWORD BEST PRACTICES

DOVE TECHNOLOGIES

There's little point in using a password manager if you don't care about password best practice. If you're not on top of this already, make sure you and your entire team are doing all the right things to keep your business and its data safe. First and most importantly, everyone – and we mean EVERYONE – in your business should do regular cyber security training. Including you.

This makes sure all your people are aware of the up-to-date risks to your business and its data. It'll help them stay safe personally, as well. Your people are your frontline defense against cyber-attacks, so it really is essential that they're armed with the right tools and knowledge to help protect the business.

DOVE TECHNOLOGIES

If your people aren't following best practice, it doesn't matter how great the security tools you use are, you'll never be as safe as you should be.

Next, make sure everyone on your team uses a password manager supplied by the business (and never their own). This will give you huge control over what happens to your data when they leave.

This is especially important if your team work remotely or take company devices home. Don't ever reuse passwords, even if you're using a password manager. You should make sure passwords are long and complex. They can be randomly generated by most password managers, and this will give you the highest level of security.

DOVE TECHNOLOGIES

PASSWORD MANAGERS

Which one should you use?

DOVE TECHNOLOGIES

LastPass

Cloud-Based

Pros

- Free trial available
- Unlimited passwords
- Automatically syncs between all devices
- Form Autofill (Automatically fills out logins, credit card info, and other forms)
- Dark Web Monitoring with paid plans (Monitors third-party data breaches)
- Compatible with most internet browsers and operating systems (Not compatible with Linux)
- Intuitive interface
- Can share multiple passwords with Family, Team, and Enterprise plans

Cons

- Reportedly poor customer service
- Only free for one device
- Somewhat costly paid plans
- No easy way to import databases
- Emergencies assess only for paid plans

Bottom Line

LastPass's free plan is not robust enough for most businesses. This is mainly due to their one device limit and lack of emergency access.

If you choose to go with LastPass, we recommend choosing their one of their business plans and doing a free trial to explore the service before making your final decision.

DOVE TECHNOLOGIES

Dashlane

Cloud-Based

Pros

- Free trial available for Team plan
- Unlimited passwords
- Automatically syncs between all devices
- Form Autofill (Automatically fills out logins, credit card info, and other forms)
- Dark Web Monitoring with paid plans (Monitors third-party data breaches)
- Offers password history, 2FA, and personalized security alerts with free plan
- Intuitive interface
- Can share passwords with free plan
- Premium users get unlimited VPN

Cons

- Only free for one device
- Costly paid plans

Bottom Line

We'd highly recommend giving Dashlane a try.

They have earned PC Mag's Editor Choice Award for their advanced features and overall ease of use. Not only that, but they have also won Apple's App Store Editor's Choice and Google Play's Best App award.

DOVE TECHNOLOGIES

Keeper

Cloud-Based

Pros

Because of Keeper's lack of features for free plans we will be reviewing the pros of Keeper's business plan.

- Offers price matching for quotes from competitors
- Encrypted vault for every user
- Unlimited Devices
- When you buy Keeper Business, each team member gets a free Keeper Family Plan Autofill passwords
- Training and support
- Security Audit and Reporting
- User Activity Reporting
- Two-Factor Authentication
- Retains a full history of passwords and files
- Secure password sharing and inheritance

Cons

- Only free for one device
- Free plan lacks many features

Bottom Line

Keeper is the clear winner when it comes to features and price even considering their lackluster free plan. Their business plan is only $3.75 per user/ per month.

Keeper has also won PC Mag's Best of the Year 2022 award as well as U.S News 360 2021 Review.

DOVE TECHNOLOGIES

Pricing

Here's a breakdown of the pricing for each service's business plan:

LastPass

$4.50
per user / month
billed annually

$54 per year

Dashlane

$8
per user / month
billed annually

$96 per year

Keeper

$3.75
per user / month
billed annually

$45 per year

DOVE TECHNOLOGIES

Master Password

Once you've chosen a password manager for your organization, each user will need to create a master password. This is the password that allows you to log in to your password manager.

For this password, it should be easy to remember, but hard to guess. We recommend a phrase in which you take the first letter of each word and use that as the letter portion of your password. For example, "Neon Blue Palm Trees Are Rare There Are Only 2" would become "Nbptartao2".

Imagine if you had to remember a password like that for every website, application, and device?

That's why we highly recommend a password manager, to make your life easier and more secure.

DOVE TECHNOLOGIES

THANK YOU FOR READING!

DOVE TECHNOLOGIES