

1Passw@rd

# Beginner's guide to password managers





# Introduction

We all have passwords to deal with. So. Many. Passwords. How on earth are you and your team meant to remember them all?

You could use the same password for everything, but that's a huge security risk because if any site you use gets hacked, all of your business-related accounts are suddenly at risk. Alternatively, you and your coworkers could make physical password notebooks. But jotting down hundreds of secure passwords like "M#A]E?vXWQ@Es8EiGJd=" is hardly practical. And typing them out every time you and your colleagues want to sign in to an online account is really boring.

# Enter the password manager



## It will help you to:

- Create strong, unique passwords that keep your team's accounts secure
- Share passwords securely with team members and trusted partners
- Save and fill everything else that's important to your business, including credit card numbers and addresses
- Update weak and reused passwords
- Quickly change passwords that have been exposed in data breaches
- And so much more!



## In this beginner's guide, you'll learn:

- How a password manager works
- Why you need a password manager
- What to consider when choosing a password manager
- The best way to roll out a password manager in your organization

Sound good? Let's get started. 

# How a password manager works

"Qwerty". "123456". "Password". These passwords might be easy to remember, but they're also dead simple for an attacker to figure out. To stay secure and protect your company's most sensitive data, every account needs a strong and unique password. Upper and lowercase letters, numbers and symbols – the whole deal. [Machine-generated, complex passwords](#) are much harder for attackers to guess. But few people in the world can memorize one of these passwords, let alone hundreds of them.



**With a password manager like 1Password, this problem disappears.** It can create strong, hard-to-hack credentials for all your team members, keep them safe and organized, and then instantly drop them into login screens when needed.

## How does this work in practice?

01

First, you'll create an account password. **This is the only password you'll need to remember.**

**02** You'll then download your password manager's associated apps or browser extensions.

**03** Once you've signed in to these, they'll sit in the background and offer to save your passwords when you sign in to your online accounts.

A password manager will also offer to create new, secure passwords when you:

- Register for a new account online
- Update the password for an account you already own

**04** The password manager will also save the website's URL alongside your username and password. That way, it knows exactly when to pop up and autofill your saved passwords!



**Now, you don't have to remember any of the passwords for your online accounts.**

You simply click, and your username and password fill automatically. And all your data syncs securely and automatically across your devices.

# How a password manager makes your life easier

Modern life is complicated. You have enough to remember and mentally juggle without throwing hundreds of complicated passwords into the mix. With a password manager like 1Password, you and your team can simplify your digital lives and sign in to any app or website with a single click.

## Here are just a few of the benefits



### **You'll never forget a password again.**

With a password manager, you only have to remember one password – the one that protects all of your saved credentials. That means less stress and more time for the things that truly matter in your life.



### **You'll be more productive.**

A password manager will save you and your team time by autofilling saved passwords, including logins you can securely share across your team. It might only take a few seconds to type out a password, but consider how many times you enter a password every day, week, month, and year. Then multiply that number by the number of people in your company.



### **You'll save your company money.**

As the age-old saying goes, time is money. If everyone is more productive, you'll save your business some cash in the long run. A password manager will also protect you against expensive and brand-damaging data breaches (more on these a little later).

# How a password manager makes your team more secure

A password manager won't just make your team's life easier – it'll also help everyone be more secure. Now, you might be thinking: "Okay, I've read about various hacks in the news, but a criminal would never target my business, right?"



**The truth is that cybersecurity isn't a luxury – it's a necessity.**

That applies to any business, regardless of your headcount or the industry you operate in.

[Criminals are targeting companies of all sizes](#), so it doesn't matter if you're a tiny startup or a multinational corporation with offices or factories scattered all over the world.

It's true that cyber attacks are always evolving. But the largest cause of data breaches hasn't changed. Most criminals exploit "[the human element](#)" – that means the vulnerability wasn't a tool or line of code, but a person. And in most cases, that person doesn't even realize they've made a mistake.

These slip-ups usually involve weak, reused, or mismanaged passwords. Password attacks doubled to [nearly 1,000 per second in 2022](#), according to research by Microsoft.

And if an attacker gets hold of one employee password, they'll often check whether it can be used to access other accounts – along with data stored on them. Even if they use different passwords, [68 percent of internet users in the United States](#) keep them similar enough to guess.

## Here's how a password manager helps:



**A password manager makes it easy for everyone to create strong passwords.** A password manager like 1Password will generate strong passwords that are essentially impossible for an attacker to figure out with a brute-force attack.



**A password manager makes it easy for everyone to use unique passwords.** Every account should also have a unique password. Here's why: Imagine you signed up for a new app. Then, six months later, it was breached and every user's password was leaked onto the internet. If you use the same password for everything, a criminal could discover your leaked password and then try to use it to access other accounts you own.



**A password manager will help you and your team avoid phishing attacks.** A password manager will only offer to autofill your password on websites with the correct URL. So if you clicked on a link that sent you to a fake but seemingly authentic website, you would notice that your password wasn't autofilling automatically. This would force you to look at the website's URL and close the tab before sharing your username and password.



**The best password managers store more than just passwords.** Some will let you save credit cards, addresses, software license keys, and everything else that's important to your growing business.



# What to consider when choosing a password manager

You have choices when it comes to password managers. The first one is easy:

**"Do I need one?" Yes.**

Your browser's built-in password manager is [simply not secure enough](#) for today's threats. So the next step is to research the different standalone options on the market and figure out the best one for your company's specific structure, budget, and needs.

## Here are some factors to consider when choosing a password manager:

- The number of seats you will need, and your projected headcount growth
- How the password manager [promises to handle your data and privacy](#)
- Compatibility across the different browsers and devices your organization uses
- The ability to store different types of data
- Reporting features that can help identify weak passwords, or data that's been compromised in a breach
- The cost of different plans and how that matches up with your budget

# Why you should choose 1Password



Over 100,000 businesses including Slack, GitLab, and Under Armour use 1Password to protect their corporate accounts and data. Why? Because it's the password manager that helps them secure their staff at scale.

## Here are 13 reasons why 1Password is the world's most-loved password manager:

- 01 1Password makes it easy for everyone to create strong, unique passwords.** All of your team members can learn and master 1Password, regardless of their role and level of technical expertise.
- 02 1Password works on all of your team's devices, and every major web browser.** Use a mixture of Macs and Windows PCs? iOS and Android? Linux machines and Chromebooks? We've got you covered.

- 03 **1Password's intuitive design makes it simple for everyone to use.** If an app is confusing, people won't use it. That's why design is a top priority at 1Password.
- 04 **1Password [can be used as an authenticator](#) for sites that support two-factor authentication (2FA).** That means you and your team won't have to waste time opening your email or a standalone authentication app to sign in to your online accounts.
- 05 **1Password can protect other kinds of data, including credit card numbers, software license keys, and [developer secrets](#).** It can also store server information, medical records, driver licenses, and more.
- 06 **1Password is a safe place to store documents, [secure notes](#), and [other important files](#).** You can even format your notes in Markdown, a popular and lightweight markup language.
- 07 **1Password [has never been hacked](#).** We're [regularly audited by independent security firms](#). We also increased our top bug bounty reward [to \\$1 million](#) in 2022.
- 08 **1Password will alert you to password breaches and other security problems.** [Watchtower](#) integrates with [Have I Been Pwned](#) to see if any of your passwords have appeared in data breaches. It also flags weak and reused passwords.

- 09 **1Password makes it easy for administrators to control who has access to what.** Use [custom groups](#) and [shared vaults](#) to make sure that everything is kept on a need-to-know basis.
- 10 **1Password's [Travel Mode](#) will keep your data safe while you cross borders.** It lets you temporarily remove vaults that contain sensitive information from your devices.
- 11 **1Password Business gives everyone on your team [a free 1Password Families membership](#).** So your team can protect their loved ones and develop good security habits at home, too.
- 12 **1Password helps your team with robust training resources.** Learn with our free [1Password University courses](#), [Tiny Tutorials webinars](#), [downloadable guides](#), and more.
- 13 **1Password offers unrivaled support to help your team succeed.** Get help whenever you need it with 24/7 email support, [an extensive support site](#), and a [forum](#) that lets you talk with 1Password staff and customers.

# Tips and tricks for rolling out a password manager at work

Choosing the right password manager is half the battle. The other half is getting your employees to actually use it.

A password manager is most effective when everyone is using it to create, store, and share passwords at work. Your leadership team – with help from your IT department, if you have one – are responsible for:

- Providing employees with robust security tools, like a password manager
- Teaching employees how to use those tools
- Creating a culture where everyone feels empowered to develop their security skills



Start by reminding employees that using a password manager isn't just about security. **It's also a tool that will reduce stress, save them time, and boost their productivity.**

Use company onboarding to teach new hires about your password manager, and the benefits of using it properly in the workplace. If you're rolling out a password manager for the first time, you could also sit down and have a similar conversation with your existing employees. This will help reinforce the tool and nurture a culture of security in your company.

## To make your rollout a success, you could also:



### **Gamify involvement.**

Offer rewards or recognition for employees that use a password manager as intended.



### **Schedule regular check-ins and training sessions.**

These could cover password management and other security skills, with incentives for attending and passing a quiz.

When everyone's playing their part and contributing to a healthy culture of security, work will become both safer and easier. A password manager can be an asset in improving employees' day-to-day happiness and productivity, and as a result, help protect your business and its customers.

# The bottom line

Passwords are a pain. But with a password manager like 1Password, you can protect all your online accounts with strong, unique passwords. And then sign in to any website or apps with a single click. No more typing out passwords, or selecting the “forgot your password” option at the login screen.

## **It's security made simple.**

A password manager is also essential for any modern organization. Say goodbye to password spreadsheets and Post-It notes, and endless copy and pasting. With an enterprise password manager like 1Password, you can securely share business-related passwords and other sensitive data with your coworkers. You'll also get a bird's-eye overview of your company's security health from one easy-to-read dashboard.