1Password

Effortless, secure password management for startups

1Password is the world's most loved password manager. By combining industry-leading security and award-winning design, 1Password protects startups by making it easy to create, use, and share strong passwords.

With **43% of breaches involving small businesses**, startups must prioritise security from day one. Here's how 1Password can help:

Key benefits

Easy to roll out.
1Password is easy to deploy yourself, but if you'd like to and our business support team is on hand to help. They also provide training, demos, and extensive support documentation so that you can focus on building your business.

Grows with your business.
1Password Teams is a secure, scalable, and easy-to-use password manager that works for businesses of every size — from startups to enterprises. As your business grows, 1Password grows with you.

Tried and trusted.
1Password is trusted by 50,000 businesses to secure their data and is the highest rated password manager on Trustpilot.com.

Cost-effective but not a compromise.
1Password is packed with powerful security tools that guard against costly breaches, **80% of which** can be traced back to weak and compromised credentials.

A breach is a huge blow to any business, especially to startups, who may struggle to cover fines or recover their reputation.

- *1Password protects your business by making it easy for employees to create and use strong passwords.*
- *Colleagues can securely share passwords and other important information, reducing the risk of them using insecure methods like email and instant messenger.*

- *Watchtower alerts for compromised websites and vulnerable passwords so you can take action to stay secure.*

Tools that give you control.
Getting projects off the ground quickly is essential when you're starting out. With 1Password you can Instantly deploy, grant and revoke access to shared vaults. Securely add new team members and recover locked-out user accounts just as quickly.

Secure teams are productive teams.
When security is easy and convenient, employees are more likely to embrace it. As you take on new employees 1Password will fit seamlessly into their workflow and help build good security habits right from the start. When everyone uses 1Password, your risk goes down — and productivity goes up.

Always connected.
1Password is available for Mac, Windows, iOS, iPadOS, Android, Linux, and Chrome OS. It works in Safari, Chrome, Firefox, Brave, and Microsoft Edge. 1Password syncs seamlessly across devices too, so employees always have access to their data.

Share with freelancers and guests.
Startups often need to work with freelancers and contractors on a temporary basis. With 1Password, you can give guests limited access to vaults while they're working with you.

More than a password manager.
There is a lot to keep track of when you're starting a new business. 1Password provides a single safe place to keep everything important. Store and secure important documents, bank details, credit cards, passport numbers, insurance details, and more.

Private by design.
Only you can access your data. We don't use it, we don't share it, and we don't sell it. You're our customer, not our product.

About 1Password Teams

- Use the password generator to **create strong, unique passwords for every account**.
- **Fill usernames, passwords, credit card numbers, and addresses** into websites and supported apps.
- Unlimited shared vaults and item storage. Store and organize information in more than a dozen categories, including logins, credit cards, addresses, notes, documents, passports, driver licenses, and software licenses.
- **Import data into 1Password** from applications like Chrome, Dashlane, LastPass, SplashID, and Roboform.
- Access your data in the 1Password apps, even when you're offline.
- **Use 1Password as an authenticator** for sites that offer two-factor authentication.
- Get 1GB secure document storage per person.
- Use Duo integration for business-wide multi-factor authentication.
- Use **Watchtower** to find out about password breaches and other problems with the items you've saved in 1Password.
- Manage employee access with **unlimited shared vaults and vault permissions**.
- Admin controls to view and manage permissions.
- Use **account recovery** to recover access for team members that can't sign in to their account.
- Use **Managed Travel Mode** to remove sensitive vaults from employees' devices before they travel.
- **Add multiple accounts to the 1Password apps** so you can see all your data in one place.

- Restore deleted items or revert to a previous version of an item with one year of **item history**.
- Share vaults with people on a limited basis with 5 free **guest accounts**.
- Get help and deployment advice from our dedicated business support team.
- 1Password is GDPR compliant, and offers **regional hosting** and pricing in Canada and Europe for data residency requirements.

  1Password Teams is $3.99USD per person per month, paid annually, and you can try it free for 30 days. Discounts are also available for education providers and non-profit organizations.

Watchtower

Watchtower tells you about password breaches and other security problems with the items you have saved in 1Password.

Compromised Websites:
Logins for websites where a security breach has been reported, and you haven't changed your password since the breach.

Vulnerable Passwords:
Items with passwords that have been exposed in a data breach according to haveibeenpwned.com.

Reused Passwords:
Items that share the same password.

Weak Passwords:
Items with passwords that are easy to guess.

Unsecured Websites:
Logins in which the first website field starts with http://. Passwords entered on these sites will be sent in plain text and could be intercepted.

Two-Factor Authentication:
Logins for websites that support two-factor authentication, but don't have a one-time password.

Expiring:
Items that have already expired, or will expire in the next 2 months (9 months for passports).

Security & Privacy

1Password is **secure by design**. The information you store in 1Password is end-to-end encrypted using 256-bit AES encryption. Only you hold the keys to decrypt your data.

- Your Master Password and Secret Key combine to create the full encryption key that encrypts everything you store in 1Password.
  - *Only you know your Master Password. It protects your 1Password data on your devices.*
  - *Your **Secret Key** is created locally and only stored on devices you authorize. Only you have access to it. It protects your data off your devices, so someone who attempts a brute-force attack on our servers won't have enough information to decrypt your data.*
  - *Your Master Password and Secret Key are never transmitted over the network.*
- 1Password offers **two-factor authentication** for an additional layer of protection. Use authenticator apps and security keys, or Duo for your business account.
- Unlock 1Password with biometrics: Face ID, Touch ID, Windows Hello, and Fingerprint Unlock.
- 1Password is designed to keep your data safe in other ways:
  - *Can remove 1Password data from your clipboard after a time you specify.*

- *Only fills your details if your browser is signed by an identified developer.*
- *Protects you from phishing by only filling credentials on the sites where you saved them.*
- *Uses secure input fields to prevent keyloggers and other tools from knowing what you type in 1Password.*
- *Only displays or fills data when you tell it to.*

- Our security is **regularly reviewed by other security experts**:
- *1Password is SOC 2 Type 2 certified*
- *Ongoing bug bounty program on BugCrowd with a maximum reward of $100k.*
- *Penetration tests and code reviews*

- 1Password was designed with a deep respect for your privacy. Your data is yours, and we don't use it, share it, or sell it. We only collect information necessary to provide our services and help you with troubleshooting. We never share any personally identifiable information with third parties.