



1Password

Page **Discussion**

Read Edit Edit source View history Tools



Article status notice: This article has been marked as incomplete

This article needs additional work for its sourcing and verifiability to meet the wiki's [Content Guidelines](#) and be in line with our [Mission Statement](#) for comprehensive coverage of consumer protection issues.

This notice will be removed once sufficient documentation has been added to establish the systemic nature of these issues. Once you believe the article is ready to have its notice removed, please visit the [Moderator's noticeboard](#), or the [discord](#) and post to the [#appeals](#) channel.

[Learn more](#) ▼

1Password is a multi-platform subscription-based **Password manager** developed by **AgileBits Inc.** One of the unique elements of this password manager is the combination of a master password with a second secret key generated on-device (i.e., not in the cloud). Unlocking a user's vault therefore requires **both** pieces of information to decrypt and access. Conventional **Two factor authentication** using either software tokens or hardware-based tokens (e.g., **Yubikey**, **Google Titan**) can be added to further secure a vault. 1Password is not open source and not self-hostable.

Beyond passwords, 1Password is capable of storing myriad site credentials including one-time codes, emails / user names, and additional notes. A user can also choose a preferred single sign-on service to login.

Consumer impact summary [\[edit \]](#)

[edit source](#)]

Freedom [\[edit | edit source \]](#)

Users can import existing passwords from other managers and export passwords and other content in formats suitable for importing into other managers. 1Password is not a walled-

1Password



1Password

Basic Information

Release Year	2006
Product Type	Software,Password Managers
In Production	Yes
Official Website	https://1password.com/ ↗

garden. Allowing the subscription to expire places an account in a read-only state, allowing the user to download their passwords and other saved content.

"You can export your 1Password information at any time. If you discontinue payment, your account will enter a frozen (read-only) state that still allows you to retrieve and export your information. Your export will be limited to the information you saved in 1Password. We can't guarantee that vault permissions, group structures, and other details about relationships between people and information are included."^[1]

Privacy [\[edit | edit source \]](#)

Extracted directly from the privacy policy,

"We'll never lock you out of your 1Password account, but we're unable to decrypt it for you."^[1] (implies anything in it is hidden from the company, which, considering this is a password manager, is a very good thing)

"You have the right to know what we know. You have the right to know what we know about you and see how we handle that information. If you make such a request, you'll receive a screenshot of what we can see about you in our systems. To protect customer privacy, these requests will be carefully authenticated beyond demonstrating control of the registered email address." (expect to be any identifying information you have to provide in order to use the service such as email, name, address, payment information)

User security [\[edit | edit source \]](#)

Users should be aware that using password manager browser extensions increases their vulnerability to clickjacking^[2] where the autofill feature of password managers is abused to trick the password manager into leaking user credentials and other sensitive details.^[3] It is always best practice to copy in these elements on trusted pages manually.

Business model [\[edit | edit source \]](#)

Subscription based, has a strong emphasis on enterprise credential management, especially for secret management for software development (e.g., SSH keys, authentication tokens, API keys, etc.).

Market control [\[edit | edit source \]](#)

This section is incomplete. This notice can be deleted once all the placeholder text has been replaced.

1Password claims on its website that it is industry leading.

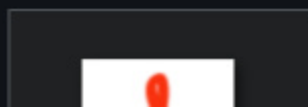
Password managers are pretty much a dime a dozen these days, highly competitive.

Incidents [\[edit | edit source \]](#)

This is a list of all consumer protection incidents related to this product. Any incidents not mentioned here can be found in the [1Password category](#).

1Password Okta instance breach, discovered (29 Sept 2023) [\[edit | edit source \]](#)

1Password published a blog post disclosing an internal investigation of the breach.^[4] It largely appears one of the attackers actions triggered an email to a member of the IT team who acted swiftly to contain the breach. The company reported user data was not exfiltrated or decrypted.





PDF document report

See also [edit | edit source]

- [Bitwarden](#)
- [LastPass](#)

References [edit | edit source]

- ↑ 1.0 1.1 "About 1Password and your privacy" . *1Password Support*. 2025-02-27. Retrieved 2025-09-05.
- ↑ Toulas, Bill (2025-08-20). "Major password managers can leak logins in clickjacking attacks" . *Bleeping Computer*. Retrieved 2025-09-05.
- ↑ Naprys, Ernestas (2025-08-21). "Major flaw affecting password managers: they autofill credentials for attackers" . *Cybernews*. Retrieved 2025-09-05.
- ↑ Canahuati, Pedro (2023-10-23). "Okta Support System incident and 1Password" . *1Password Blog*. Retrieved 2025-09-05.

Categories: [Articles in need of additional work](#) | [Articles with verification concerns or other deficiencies](#) | [1Password](#)

This page was last edited on 8 September 2025, at 06:26.

Content is available under [Creative Commons Attribution-ShareAlike 4.0 International](#) unless otherwise noted.

[Privacy policy](#) [About Consumer Rights Wiki](#) [Disclaimers](#) [Mobile view](#)

