David Irvine

Technical Writer HQ - capstone project July 2022

Email: david.irvineakamarv@gmail.com

Table of contents

[R&D] Q3 - Exploring free password management solutions

The problem

The National Cyber-Security Agency recently published the findings of its 2021 password security survey – we are concerned.

It found that 85% of people use variants of the same passwords. The survey also reports that people are *still* using pen and paper. A large number are also unconvinced their data is any safer with password managers than it is with them – they don't trust us.

People realize the risks involved with poor password hygiene, but they continue to do it anyway.

The purpose of this report is:

- To increase public awareness of Bitwarden password manager.
- To align with our values.

Proposed solution

Bitwarden must aim to provide the most comprehensive, free password management solution available.

Each personal account will include:

- Unlimited passwords
- Unlimited devices
- All core functions (see feature specifications for full list)
- Vault sharing (one other user)
- Always free

Business and family account feature sets will remain under premium subscription but at a reduced rate of $10 for the first year.

We project that this strategy will increase our share of the password management market by up to four percent annually.

Our values

Alone, a free Bitwarden vault does not guarantee our success in the password management industry. Nor will it alone increase public trust in password management solutions. It does however align with our open-source values! A free Bitwarden vault with such an extensive feature set can positively impact public perception of the Bitwarden brand and its modern internet security policies.

Bitwarden's mission is to create a world where no one can be hacked. Making a Bitwarden vault available to all users echoes our values, promotes our personal responsibility to the community, and helps raise public awareness of Bitwarden's open-source approach to password management.

Final thoughts and next steps

Public trust can be more easily attained when the public realizes the extent to which their data is encrypted. The truth is user data is incomprehensible, even to Bitwarden. This "truth" has market value, and it can be leveraged to increase public confidence in our privacy policies and our serious approach to data security.

We recommend that campaigns begin to promote Bitwarden's mission statement. Social media platforms and blogs are to be targeted as grounds to promote use cases and user journeys. Bitwarden's security infrastructure is to be demonstrated and explained clearly to enhance user awareness of the cryptographic processes deployed in protecting their data.

[COO] Q1 - What we learned from the National Cyber-Security Agency's (NCSA) 2021 annual report

Used but underutilized

People are moving more of their lives onto cloud-based services, creating an exponential challenge of increasing importance for security firms. Malware, phishing scams, hackers, and data breaches all represent a continuous threat to secured and unsecured data.

Password managers coordinate login credentials and secure user data – they're the most practical and effective defense from attack. Unfortunately, they are severely underutilized, as highlighted by the National Cyber-Security Agency's 2021 password research survey.

Key findings:

Popular password management methods

Standard memorization remains the most popular way of keeping track of online passwords, followed by an assortment of low-tech alternatives. See Figure 01 for details.

Fig 01: NCSA 2021 *multiple responses permitted

Memorization	41%
Pen and paper	30%
Save in a browser	24%
Save in a digital note (plaintext)	23%
Reuse old passwords	20%
Use a password manager	8%

Reasons for using a password manager

The most-cited reasons for using a password manager emphasized their notable strengths – generating, storing, and encrypting complex codes across multiple platforms. See Figure 02 for details.

Fig 02: NCSA 2021 *multiple responses permitted

Can't remember all my passwords	71%
Apply login across multiple devices	51%
Generate/save complex passwords	45%
Manage apps with multiple logins	38%
Password encryption	34%
Ease of a single master password	24%

Reasons against a password manager

The primary reasons cited against the adoption of password management services are rooted more in unfamiliarity than in fact. Clients embrace the convenience, while skeptics question security. See Figure 03 for details.

Fig 03: NCSA 2021 *multiple responses permitted

Don't believe they're secure	63%
Not sure I need one	49%
Don't know how they work	51%
Cost too much	36%
Difficult to set up	34%
Time-consuming	24%

Will you consider using a password manager?

Respondents without a password manager were *most* worried about security. Presumably they're unaware of the extent to which encryption keeps their data protected in the rare case of breach. See Figure 04 for details.

Most of those who currently don't use a password manager *are* willing to try one.

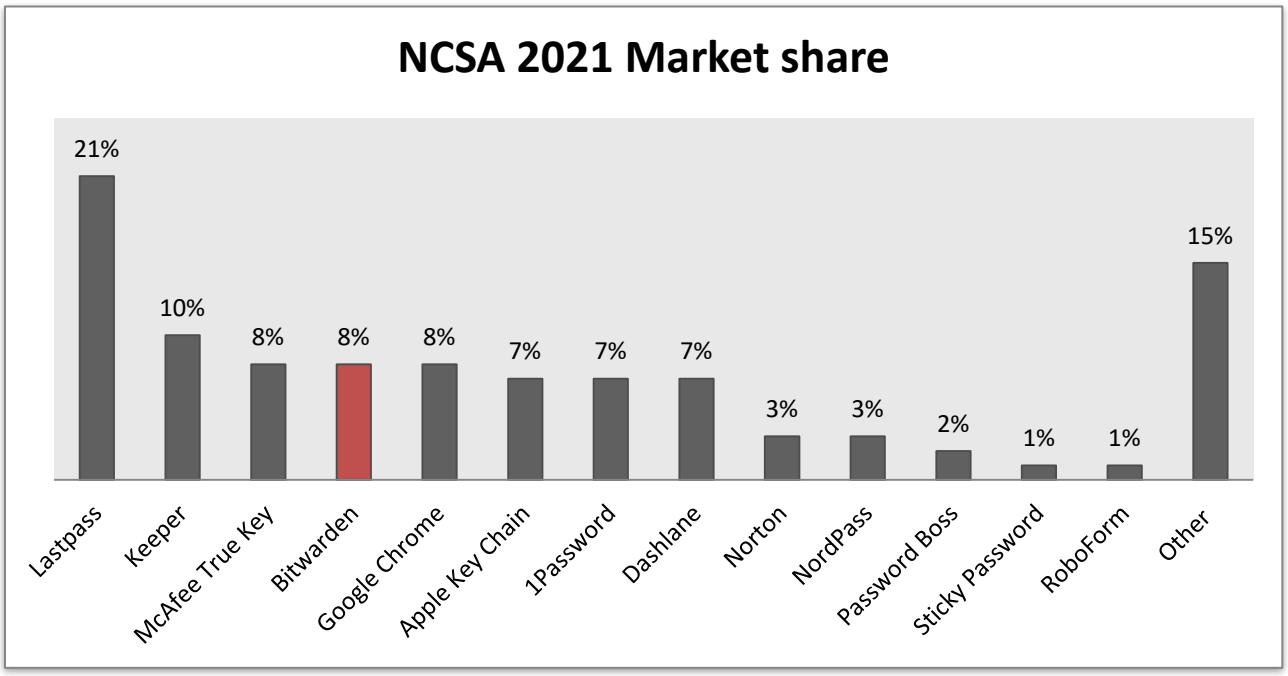
Fig 04: NCSA 2021

Yes	69%
No	31%

Market evaluation

Bitwarden's estimated 2021 market share (Q4) is up three percent on NCSA 2020. See Figure 05.

Fig 05: NCSA 2021



Bitwarden

The need for password managers

Each year more people move more of their real-world lives onto the internet. Inevitably, the more online your life becomes, the more passwords you can expect to manage.

Security experts recommend using randomly generated passwords for each account you create. The problem then is how best to manage a growing number of random passwords in a way that maintains good password hygiene - not recording and storing them somewhere in plaintext format.

If you're tired of clicking on "forgot password" or are guilty of using the same password across multiple accounts, then it's time to start thinking about getting yourself a reliable password manager.

What is Bitwarden?

Bitwarden is an open-source password management service that's user-friendly, highly secure, and includes everything individuals, teams, and businesses require in a password manager.

Bitwarden offers a free plan which includes multi-device sync, two-factor authentication (2FA), and the ability to import from other password managers, which makes it easy to try out Bitwarden at no upfront cost.

Available as a browser extension, desktop client, and mobile application, Bitwarden is a reliable and secure password manager with extensive user features.

Bitwarden highlights include:

- AES 256 encryption
- Zero-knowledge cryptography
- Auto-fill
- Password generator

Master password security – browser extension

A Bitwarden vault is protected by a single long “master” password, encrypted using PBKDF2 zero-knowledge cryptography. As a Bitwarden cloud client, your master password and email are salt-hashed twice before storage – first, on *your* device and again by Bitwarden before storage in our database.

Bitwarden only ever receives hashed versions of your password information.

Master password security – desktop client

Your master password will never be transmitted to Bitwarden servers, as all encryption is performed locally. Your master password is only temporarily stored in local RAM while it’s in use. It’s then purged from your system’s memory when the decryption of your vault has been completed.

Bitwarden will never store any plain text data on its servers or on your local devices.

Only you know what’s in the vault

Zero-knowledge hash functions are a “one way” only process. This ensures no one at Bitwarden can ever reverse engineer hashes to obtain “actual” passwords. Bitwarden will never know anything about the contents of your vault. All Bitwarden keeps is proof that you have the key – the master password. The only person who knows what’s inside your vault is you!

Bitwarden doesn't offer a master password recovery option. If you lose your password, your vault is lost. Not even Bitwarden can ever gain access to it.

Vault security

Each piece of information stored in a Bitwarden vault is encrypted using the AES-256 cipher – the same end-to-end encryption process used by the world's national security agencies to protect the highest levels of top-secret information.

Compliance

Bitwarden security and compliance policies are based on the ISO27001 Information Security Management System (ISMS). Bitwarden also meets the General Data Protection Regulation (GDPR) frameworks and California Consumer Privacy Act (CCPA) standards.

In November 2018, Bitwarden passed a third-party security and cryptographic analysis assessment performed by Cure 53. The assessment covered the Bitwarden application and back-end server systems. Bitwarden also passed a security assessment and penetration test performed by Insight Risk Consulting.

As Bitwarden is an open-source product, its source code is available online, which means it's open for scrutiny by cyber-security professionals. This ensures that Bitwarden does only what it says it does and nothing else.

Is Bitwarden safe?

Yes, by using the AES-256 cipher, hacking into a Bitwarden vault is virtually impossible. And due to Bitwarden's zero-knowledge encryption policy, not even Bitwarden has access to the data stored in its vaults.

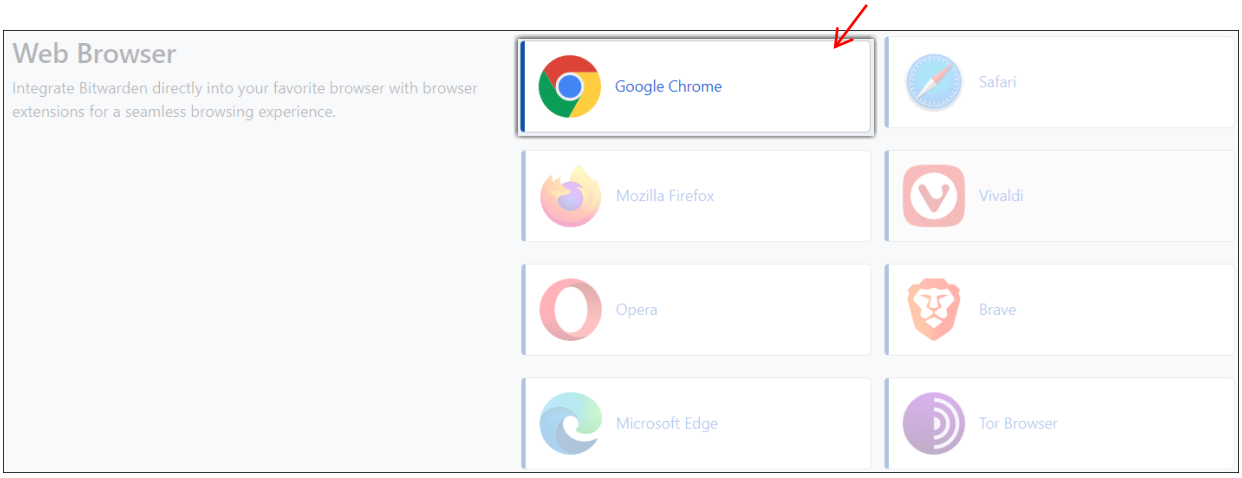
To learn more, visit Bitwarden here.

How to install the Bitwarden browser extension in Google Chrome

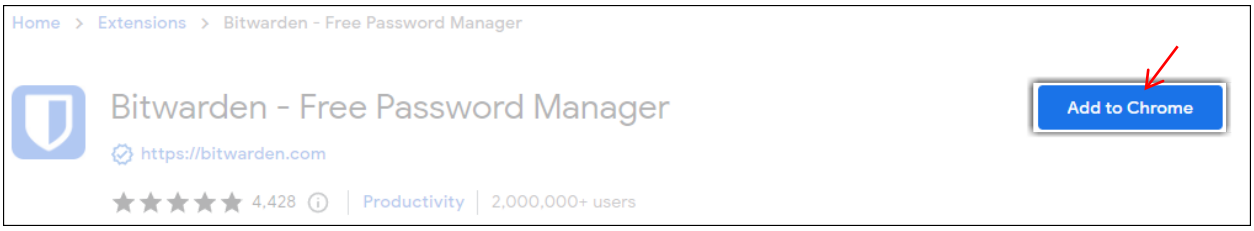
This tutorial will show you how to install Bitwarden as a browser extension.

01. Go to www.Bitwarden.com.
02. Click “Download.”

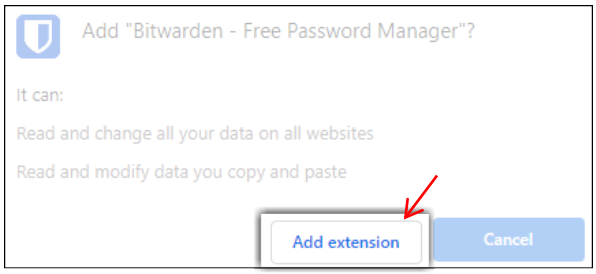
03. Scroll down, select your browser.



04. Click “Add to Chrome.”



05. Click “Add extension.”

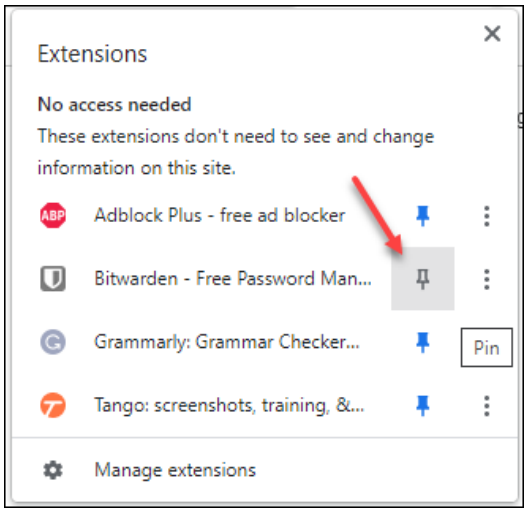


Welcome message:

How to access the Bitwarden browser extension

01. In the upper right corner of your browser, click the “Extension” button.

02. Click the grey pin-button to pin Bitwarden to your browser.



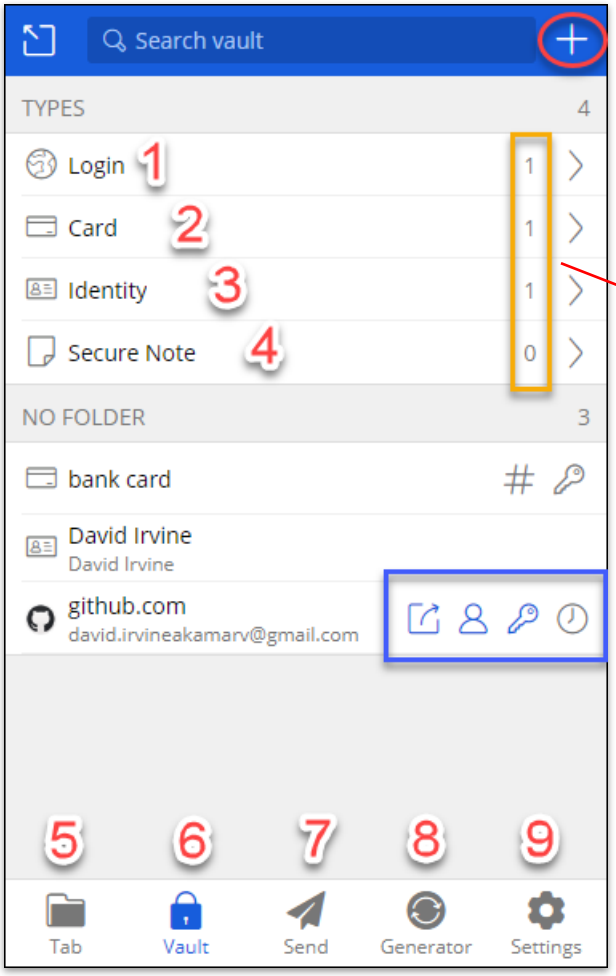
03. Bitwarden is now pinned to your browser. Click the shield to open Bitwarden.

You can now create an account.

Get started – Bitwarden vault UI quick-reference

The following UI quick-reference provides an overview of user functions available from the Bitwarden vault.

Bitwarden vault screenshot:



Click on "**+**" to add a new item to the vault.

The number of items currently stored in each tab.

Each login has quick keys:

- Launch website
- Copy username (to clipboard)
- Copy password (to clipboard)
- Copy verification (to clipboard)

Refer to Figure 01.

Figure 01: Vault UI reference	
1. Login	**List all stored logins:** - *User: select/edit/purge*
2. Card	**List all stored bank/credit card information:** - *User: select/edit/purge*
3. Identity	**Display user's personal information:** - *User: select/edit/purge*
4. Secure note	**List all stored secure notes:** - *User: select/edit/purge*
5. Tab	**Current browser window login:** - *User: add login, auto-fill*
6. Vault	**List vault contents by type:** - *User: select type*
7. Send	**Share file:** - *User: select data, add recipient*
8. Generator	**Password and username generator:** - *User: generate random password/passphrase, username/password, length, special characters, password history*
9. Settings	**Vault settings:** - *User: manage folders/sync/domain, timeout/timeout action, pin, biometrics, 2FA, import/export, about, help*

FAQs: General

I forgot my password

Sorry, but there is nothing we can do to recover your password. Bitwarden uses zero-knowledge encryption to conceal your password. This method of encryption is a one-way process. Bitwarden cannot reverse it.

To learn more about master passwords, click here.

Can I backup my vault?

Yes, you can back up your vault. Your vault data can be exported in an encrypted JSON file. Exports are encrypted using your account's encryption key and are unique to each Bitwarden user.

To learn more about encrypted exports, click here.

Can I view my password history?

Yes, you can view your password history. The last five passwords for any login item can be viewed. To do so, first, select an item and click "1," next to password history at the bottom of your vault window.

Warning! - clicking on password history will display your historical passwords in **plaintext**.

Can I print my vault data?

No, you can't print vault data directly from Bitwarden. You can however, export vault data as a JSON or .CSV file and print it from a text editor.

Does Bitwarden only store passwords?

No, Bitwarden doesn't only store passwords. Bitwarden can secure any data that can be stored in plaintext formats.

FAQs: Security

Can Bitwarden read my password?

No, Bitwarden cannot read your password. Bitwarden servers only store encrypted and hashed data. Your data is fully encrypted and hashed before leaving your local device.

For more information about how your data is encrypted click here.

Does Bitwarden support two-factor authentication (2FA)?

Yes, Bitwarden fully supports two-factor authentication. Bitwarden offers SMS, email, and third-party authenticator options free with all personal accounts. Additional options are available on premium plans.

For more information and the full list of 2FA options, click here.

Why should I trust Bitwarden?

There are several reasons to trust Bitwarden:

- Bitwarden's source code is available online and has been reviewed by hundreds of developers. Bitwarden only does what it claims to do, nothing else.
- Bitwarden routinely undergoes security audits from 3rd party security firms and individual researchers.
- Bitwarden does not store your passwords. Bitwarden stores encrypted versions of passwords that only you can unlock.
- Bitwarden uses AES-CBC 256-bit encryption for your vault data and PBKDF2 SHA-256 to derive your encryption key.

What if Bitwarden gets hacked?

Your vault and password information are *still* protected – they're encrypted by one-way salt-hashing.

Update: 2022.6.0

Note:

We have adopted a new numbering system!

As Bitwarden moves towards a near-monthly release cycle, we've decided to adopt a new release numbering system to share across **all clients**.

This release is 2022.6.0 because it's the base release (.0) of June (.6) 2022 (2022).

The Bitwarden **2022.6.0** update includes key features and usability improvements to make life easier on-the-go:

- **Auto-fill account switching (IOS)**: You can now switch between accounts during auto-fill – just tap the avatar button. Available on Android and IOS. Click here for more information.
- **Vault filtering on mobile**: You can now filter vault items on mobile devices.
- **Organization members:** You can now use premium features like 2FA when invited, you no longer need to wait on being confirmed.
- **Accessibility improvements:** You can now use an accessibility cookie to skip hCaptcha challenges (users with hCaptcha accessibility access only). This is now available on both desktop and mobile platforms. **It is not currently available to browser extension users.** It's expected in the **2022.8.0** update.
- **Notifications:** notification processes upgraded – they now run faster.

Note: No bugs reported for 232 days.

Bitwarden believes in open-source transparency. For a fully detailed view of all previous release notes and source code, visit Bitwarden on GitHub.com.

User persona

John Doe

age: **59**
residence: **London, UK**
education: **Bachelor degree**
occupation: **Civil servant**
marital status: **Married | 3 children**

"...It's difficult for me to trust my personal information to such a new company. What if they dont know what they're doing?"

John has been a civil servant for over 30 years. Recently he was the victim of a data breach - his social media was hacked. This caused substantial inconvenience and embarrassment to John, as he considers himself tech-savvy - he has been using computers for 20+ years.
John recognizes that he needs to take more care in the handling of his web credentials. Currently, John is looking at the password management solutions available to him - convenience, ease of use and reputable branding are important to John.

Comfort With Technology

INTERNET

SOFTWARE

MOBILE APPS

SOCIAL NETWORK

Criteria For Success:
To avoid further hack attacks and unwanted exposure of private information.

Needs
- To feel confident
- To be able to freely manage all aspects

Wants
- Convenience and peace of mind
- Products that integrate with his existing technology usage

Values
- Recommendations from friends
- A modern approach to security
- Transparency

Fears
- Taking too much time to set up/use
- Too complex
- Doesn't actually feel any safer with a PM service
- Too expensive

bitwarden