

# How to Safely Backup Your Password Manager

After years of relying on password managers, you know that even these trusted digital vaults are not immune to errors. When your password manager crashes or locks you out unexpectedly, backups become essential.

After years of relying on password managers, you know that even these trusted digital vaults are not immune to errors. When your password manager crashes or locks you out unexpectedly, backups become essential.

## Why should you back up your password manager regularly?

Password managers are an important part of our online presence. In addition to storing online logins, password managers have other practical uses, such as storing secure notes and sharing logins with family members. However, relying on them without a backup plan is risky.

For example, when someone's password manager suddenly crashed last year, he was lucky because he didn't store many passwords and recovered his password manager's master key fairly quickly. But those panicked hours should teach you that even the most secure password vaults aren't immune to breaches.

Technical glitches aren't the only threat. Sometimes, you can forget your master password during stressful times or if you haven't written it down.

In addition to restoring access, password backups provide practical benefits like easy migration between services and protection against ransomware attacks targeting your password manager. You hope you never need them, but having a backup available when you do is invaluable.

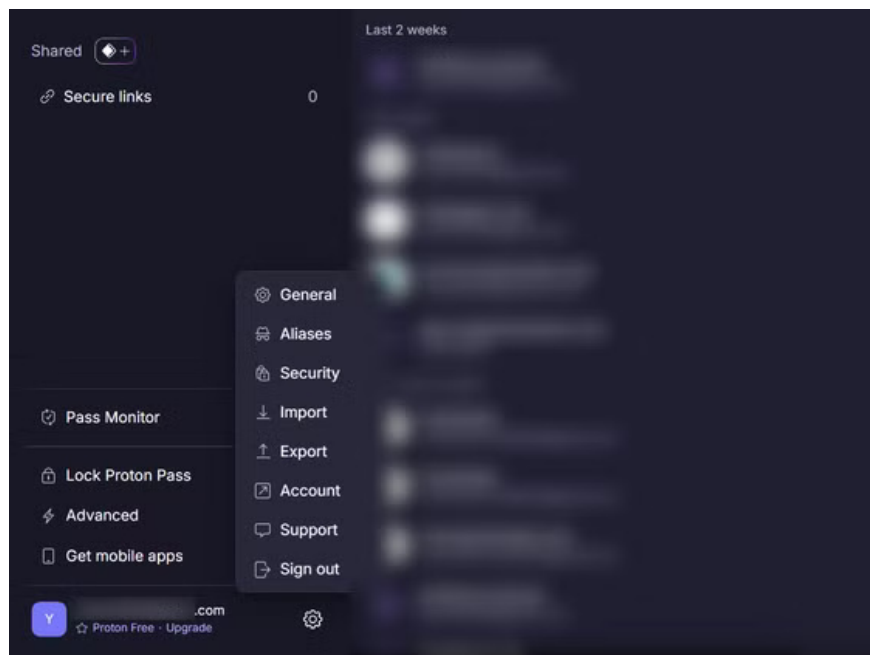
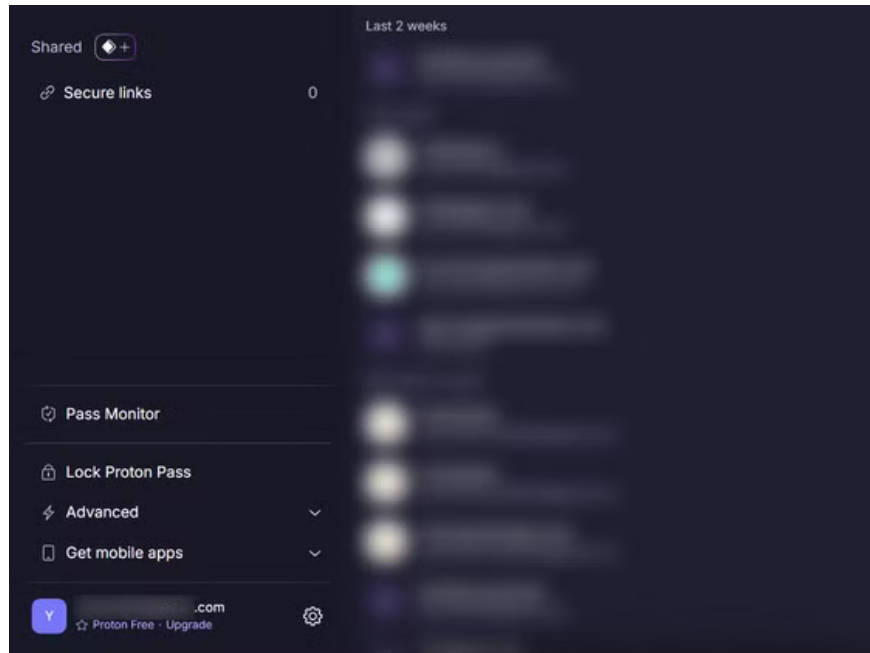
Most password managers make exporting your data simple, although the exact steps vary from service to service. After testing the export processes across four popular options, some offer a more user-friendly experience than others, and all offer ways to create offline backups of your digital vault. Here's how to secure your passwords from each service.

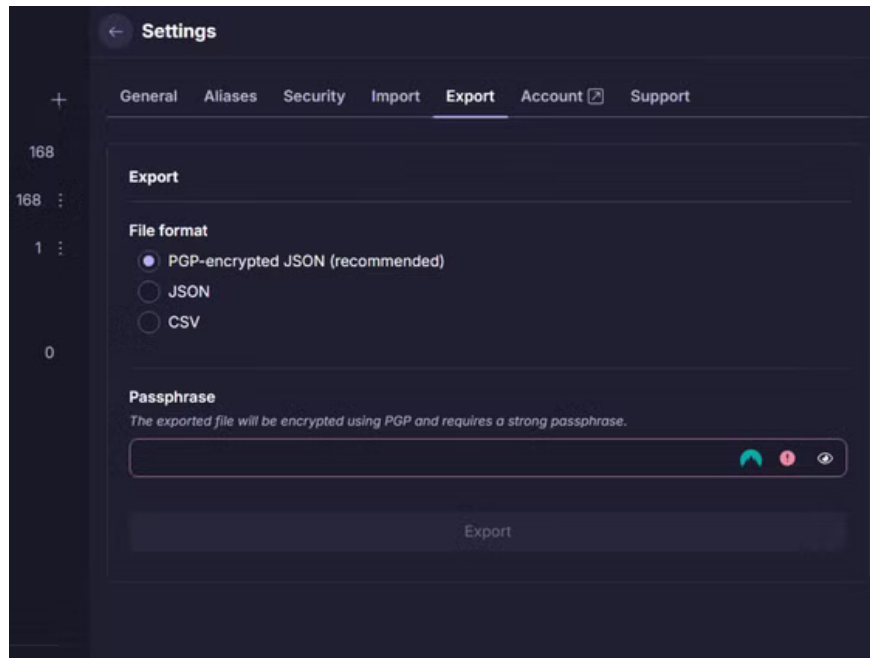
## How to export Proton Pass password vault

Many people have turned to Proton Pass as their new favorite password manager due to its emphasis on privacy. Exporting is simple, but requires the web app as the mobile app does not currently support exporting. To create a backup from Proton Pass:

[Download Proton Pass \(Free\)](#)

1. Log in to your Proton Pass account .
2. Select **Settings** in the lower left corner.
3. Click **Export** from the menu that appears.
4. Choose your preferred export format ( JSON , CSV or PGP encrypted JSON ).
5. Enter your Proton Pass password to verify your identity.
6. Click **Export** and choose where to save the file.





The exported file contains all of your login information, secure notes, and credit card information — but no attachments.

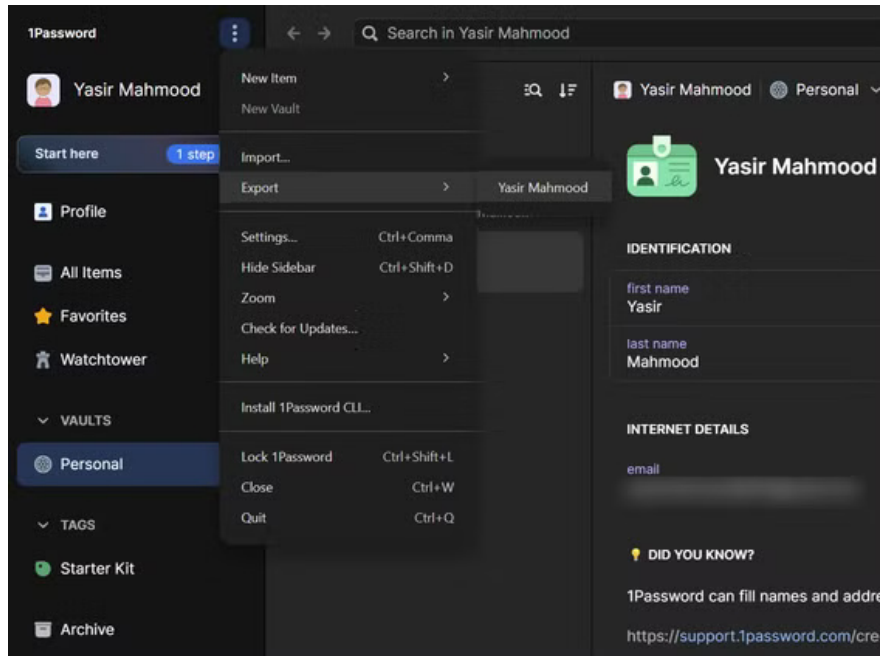
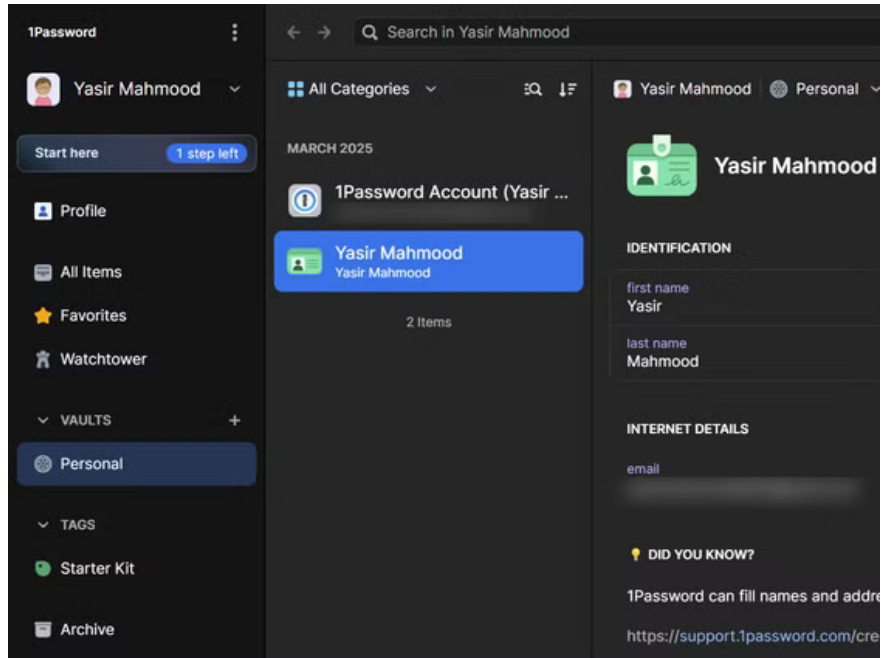
## How to export 1Password password vault

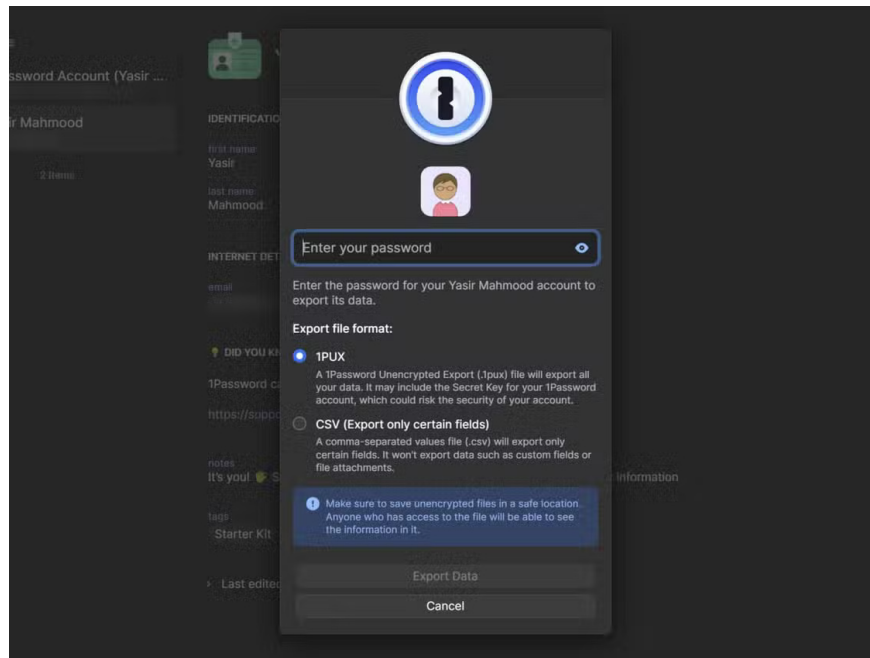
1Password offers backup options, but it doesn't encrypt exports by default—which is a concern for a security-focused tool. It allows exports in two formats: 1PUX and CSV, each with different limitations. And you'll need the desktop app to back up your passwords.

### Download 1Password (Free)

The 1PUX format is an unencrypted 1Password export file that includes all of your data. While comprehensive, it may contain your private keys, potentially compromising your account security if the file falls into the wrong hands. The CSV option is more limited, omitting custom fields and file attachments. Follow these steps to export from 1Password:

1. Open the 1Password desktop app.
2. **Click on the File** menu option (three dots) in the top left corner and select **Export** .
3. Select **All Vaults** or select a specific vault.
4. Choose the format you want (1PUX or CSV).
5. Enter your master password when prompted.
6. Select destination to save the output file.





**Tip :** If you plan on switching password managers, the CSV option offers better compatibility with other services.

## How to export your NordPass vault

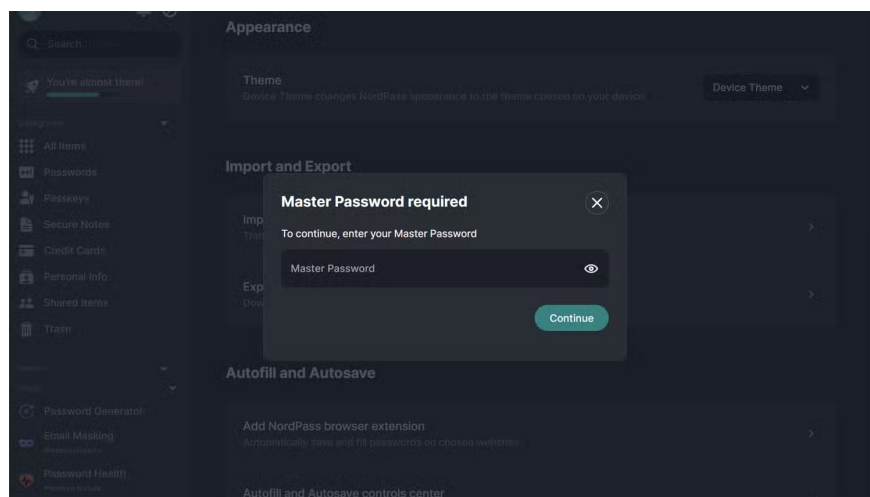
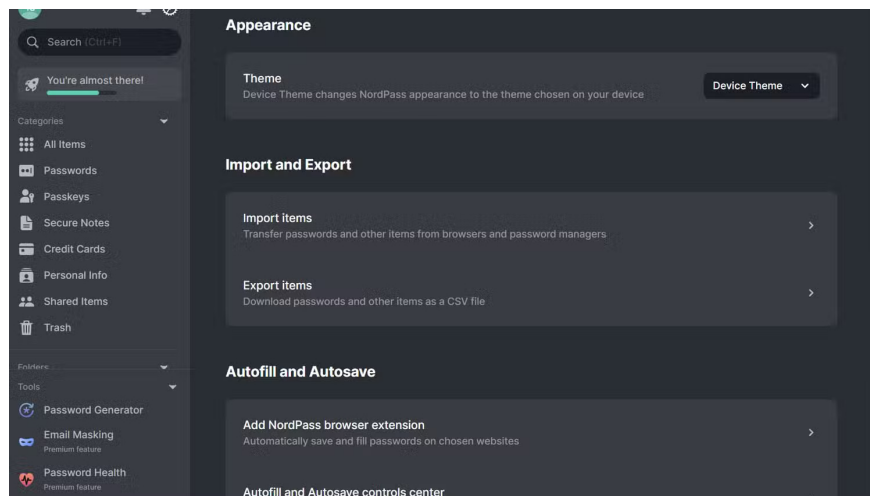
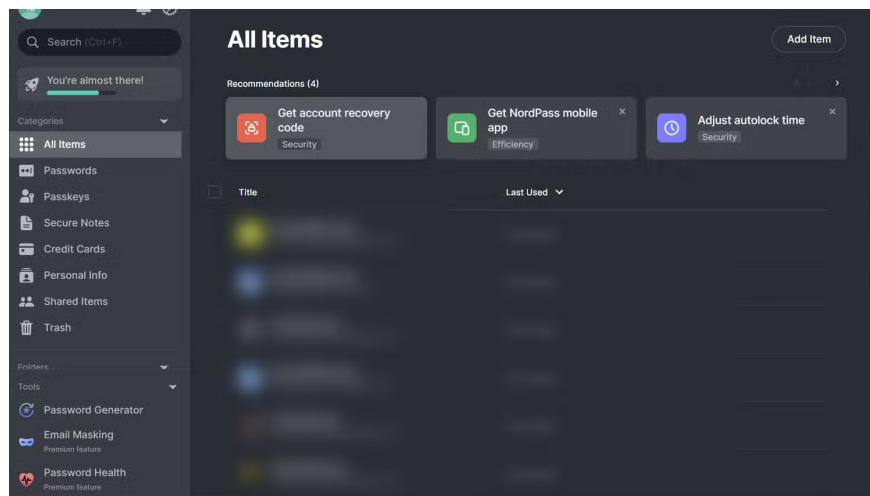
NordPass takes a simpler approach to password exporting, but has one major limitation — it only allows unencrypted CSV exports. While convenient for compatibility with other services, this format leaves sensitive data vulnerable until you secure the file.

Despite strong encryption for saved passwords, many people were disappointed that NordPass doesn't offer an encrypted export option like its competitors. And you'll need the desktop app to back up your passwords.

Download NordPass (Free)

Here's how to export from NordPass:

1. Open the NordPass desktop application.
2. Click the **Settings** icon (gear icon) in the upper left corner.
3. Select **Export items** in the **Import and Export** tab .
4. Enter your master password to verify your identity.
5. Click **Export** to create a CSV file.
6. Select a location to save the file on your device.



Remember to delete the exported CSV file from your downloads folder after you have moved it to a safe storage location.

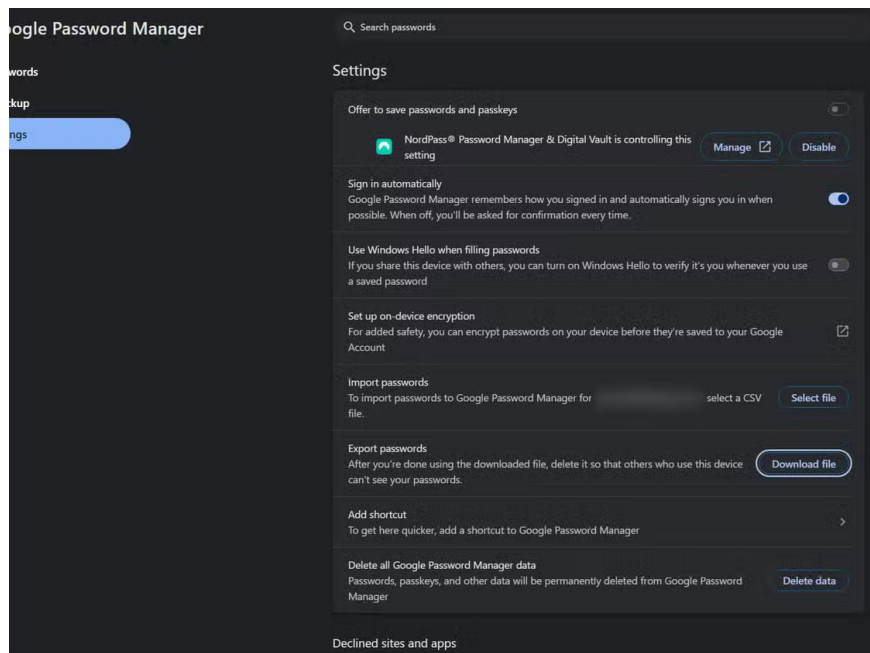
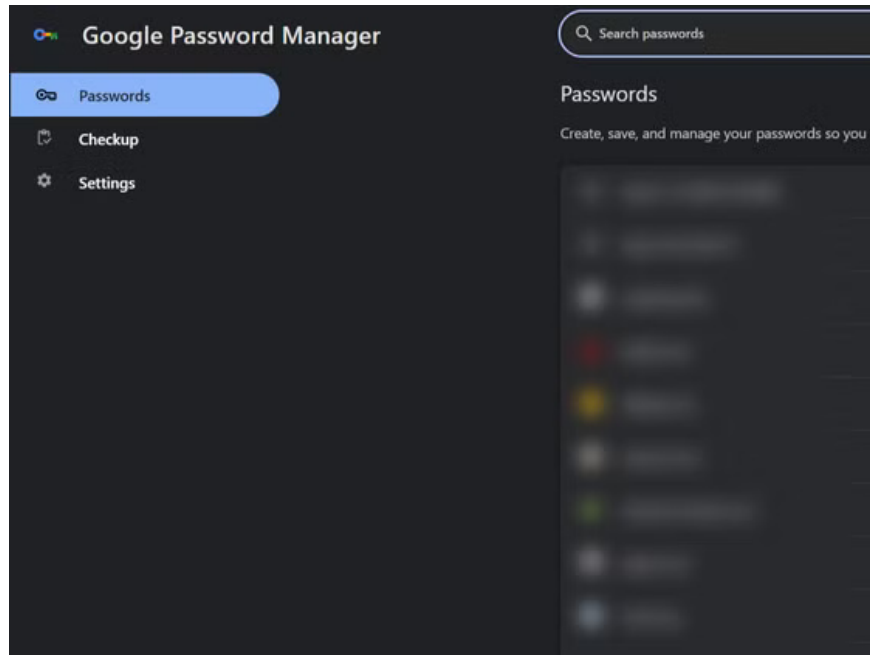
## How to export archive from Google Passwords

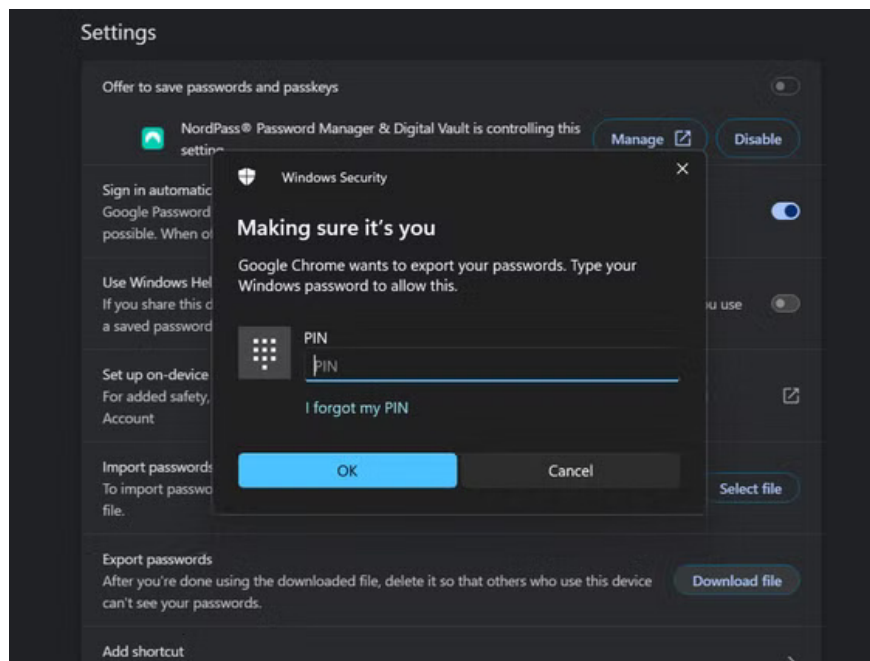
Google's password manager is probably the most accessible option for many of us because it's built into Chrome, but its export process isn't immediately obvious. Like other services, Google only offers unencrypted

CSV exports.

While convenient for storing regular passwords, Google's approach to exporting highlights why dedicated password managers often offer better security features, so you should keep others from snooping. However, backing up is easy once you know where to look.

1. Open Chrome and click your profile icon in the upper right corner.
2. Select **Passwords and autofill** (lock icon) or type *chrome://password-manager* in the address bar.
3. Go to **Settings** and select **Download file** under **Export Passwords** .
4. Verify your identity using your computer's login information.
5. Select a location to save the CSV file and click **Save** to complete the export process.





**Note :** The export includes all your saved passwords and usernames but ignores any payment methods or addresses you've saved in Chrome.

## Secure exported password data

Once you export your password vault, you hold the keys to your entire online life. This unencrypted file needs to be protected immediately—leaving it unsecured defeats the purpose of having a password manager in the first place.

When it comes to digital storage, encryption is a non-negotiable. You can protect your data with VeraCrypt to create encrypted containers for your password backups that require a separate strong password to access. Some people like to use encrypted cloud storage services like Proton Drive or Cryptomator with Dropbox, which are both secure and easy to access.

Physical storage provides another layer of protection. Consider storing your encrypted backup on a dedicated USB drive kept in a secure location. For important accounts, some security experts even recommend using a hardware security key as an additional backup method for account recovery.

Maintain multiple backup locations using the 3-2-1 backup rule: 3 copies of your data on 2 different types of storage with 1 copy kept off-site. This protects against device failure, theft, or natural disasters. Just remember to update all backups whenever you add new important accounts.

You finished reading the article "**How to Safely Backup Your Password Manager**" edited by the [TipsMake](#) team. We hope this article has provided you with many useful tech tips and tricks. You can search for similar articles on tips and guides. Thank you for reading and for following us regularly.