6 Simple Steps to Make Your Passwords More Secure

Still using 123456 or your birth year as your password? It's time to stop! Using weak and commonly used passwords is one of the main reasons why you might get hacked.

Still using '123456' or your birth year as your password? It's time to stop! Using weak and commonly used passwords is one of the main reasons you might get hacked. Luckily, you can easily upgrade your password practices with these steps!

1. Confirm the problem

The first step to better password security is admitting that your current practices may not be secure enough. But how do you know? Some signs that you have a password security problem include:

1. Using the same password for multiple accounts
2. Save passwords in a notebook
3. Include personal information in password
4. Choose a memorable password

If any of these apply to you, then your current password habits are putting you at risk. Now that you've identified the problem, it's time to make your passwords much stronger and more secure.

2. Choose a password manager

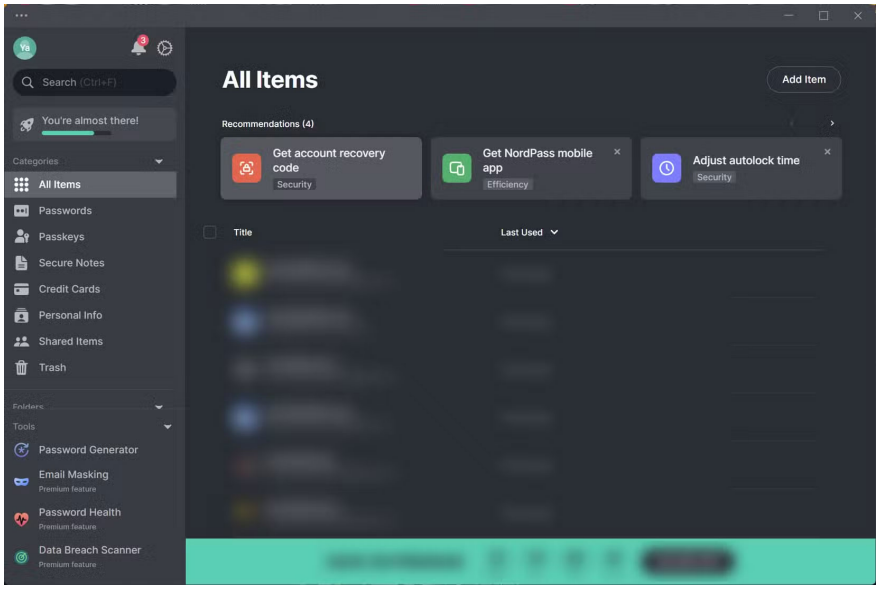
Once you acknowledge the problem, the next step is to let technology do the heavy lifting. We're no longer in the early days of the internet , when most people only had a handful of accounts. Now, you probably have dozens of online accounts, and a password manager is essential for keeping track of all those unique passwords.

In short, a password manager is an application that stores all your login information in a secure, encrypted vault. It provides a more convenient and secure way to store and generate passwords.

This will be the central place where you store passwords for all your accounts. Additionally, modern password managers can generate strong and secure passwords and include features like password sharing for added convenience.

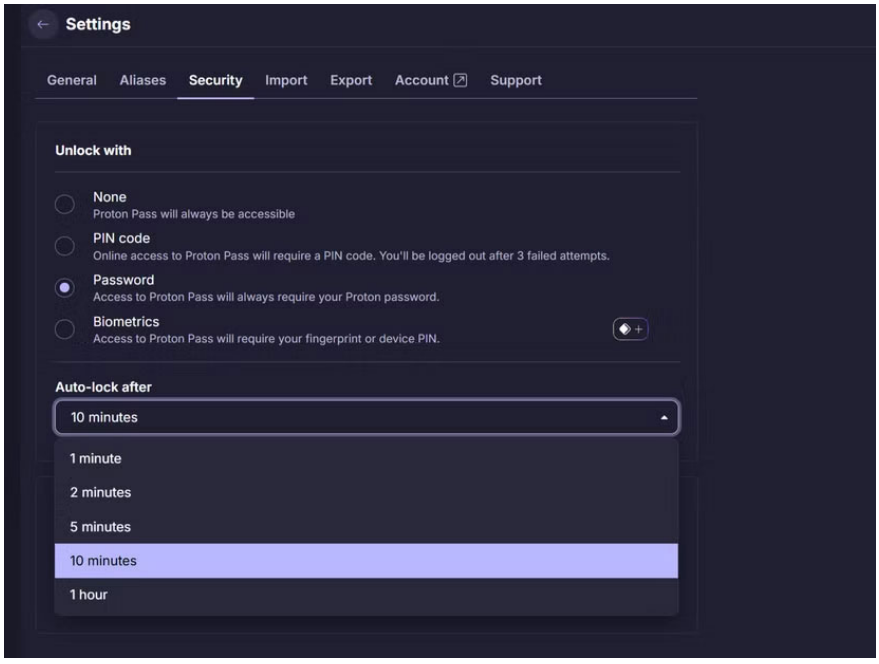
That said, there are plenty of password managers available. The most prominent options include Bitwarden , Dashlane , 1Password , NordPass , and ProtonPass — all of which offer the must-have features you need in a password manager .

3. Set up a password manager



Once you've decided to use a password manager, it's time to set it up. Start by creating a strong master password, which is the password you'll use to unlock your password manager. The master password is the password you'll need to remember, so make it long, unique, and hard to guess — no birthdays or nicknames.

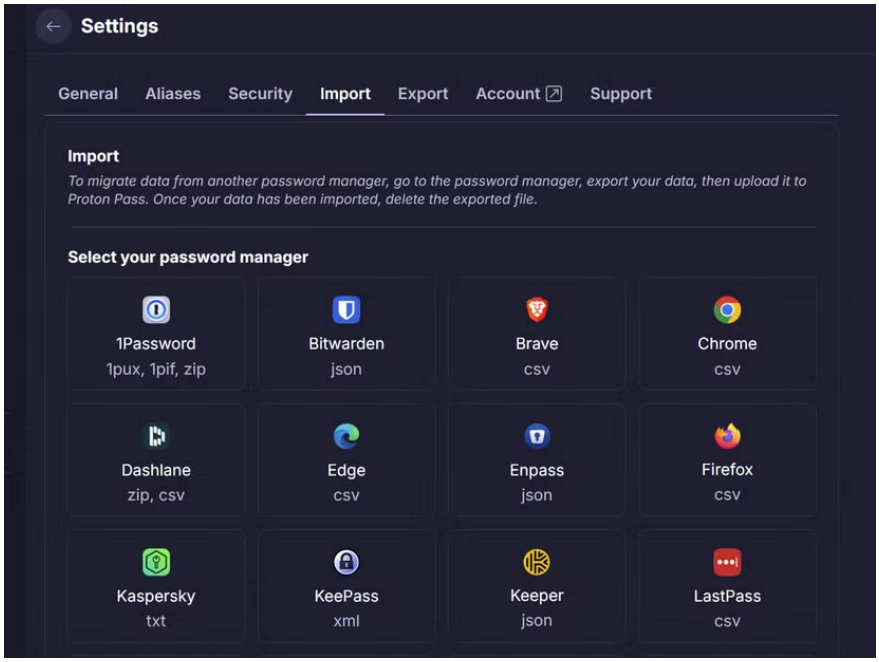
The best approach is to use a passphrase, which will help you avoid common mistakes when setting up a password manager. A passphrase is a string of words that is typically longer than the password used for authentication. Come up with a unique and memorable sentence, then add a few letters and special characters here and there to create a strong master password. For example, *1Lik3Sunshine$Over-Mountains42* is a long, memorable passphrase that includes numbers, symbols, lowercase and uppercase letters.



Be sure to set up a recovery email, which will help you regain access if you forget your master password. Finally, install password management apps on your devices. Install desktop and mobile apps, and for your

preferred desktop browser, install the extension (if available).

4. Start migrating current passwords



The best password managers offer ways to import passwords from your browser or other password managers. However, when starting from scratch, you can only add existing passwords manually.

If you have a lot of accounts, don't feel the need to add them all at once — you can move a few accounts at a time. The best approach is to start with your most important accounts, like email, banking, social media , shopping sites, and work-related accounts.

For the rest of the sites, you can slowly let your password manager automatically save your login information when you visit any of those sites and log in or sign up. Over time, your password manager will store the login information for all of your accounts. And when you reach that point, it's time to back up your password manager.

5. Enable additional security features

With your passwords stored in one place — your password manager — the next step is to beef up the security of your password vault. First, enable two-factor authentication (2FA) for your password manager.

Even if your master password is compromised, 2FA adds an extra layer of protection to keep your vault safe. Some password managers also give you the option to re-enter your master password before viewing specific passwords.

6. Maintain strong security habits

Using a password manager to store your passwords is a good first step. But it doesn't stop there. Going forward, it's essential to have a system in place to ensure the security of your storage and passwords.

This includes reviewing your passwords quarterly, updating important passwords every three to four months, and updating your password manager regularly. Some password managers also provide security analytics, also known as password vault health, to identify weak or duplicate passwords. Make sure you use them.

You should also avoid reusing passwords and use a password manager to generate strong, secure passwords.