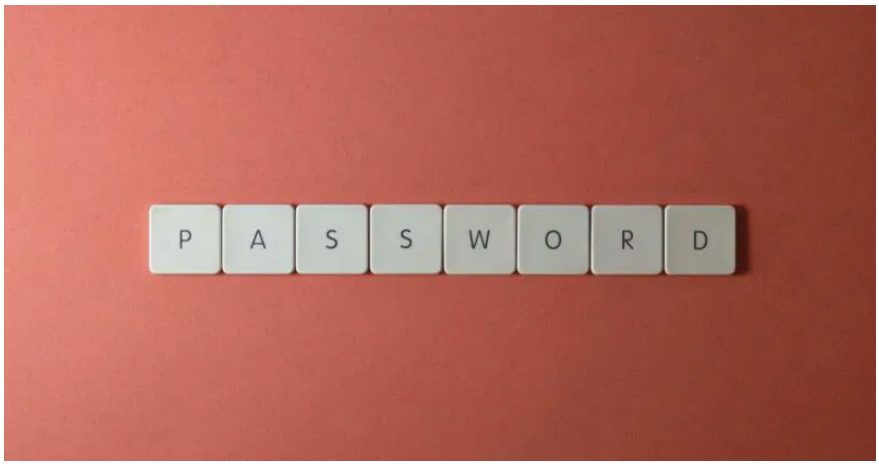
Why is storing passwords in the Notes app a bad idea?

Many people find it convenient to store passwords in note-taking apps like Evernote or Apple Notes, but this practice can put your security at risk.

Many people find it convenient to store passwords in note-taking apps like Evernote or Apple Notes, but this practice can be a security risk. Let's take a look at why note-taking apps are high-risk places to store sensitive data—and the best ways to store your passwords.

Why is storing passwords in a notes app a bad idea?

Many people write down passwords in plain text—on sticky notes or in smartphone apps—for convenience. In fact, about a quarter of us store passwords in digital notes or documents, according to data from the Pew Research Center.



Unfortunately, that convenience comes with serious security risks, as the primary purpose of note-taking apps is not to protect sensitive information, leading to a number of cybersecurity vulnerabilities. The biggest of these is the fact that most common note-taking apps are not automatically encrypted.

The lack of encryption leaves you at the mercy of your device's security. If your phone or laptop is lost or stolen (or simply unlocked in the wrong hands), all of your passwords are instantly exposed.

While you can lock your entire phone with a passcode or biometric lock, if your notes are synced to the cloud and someone gains access to your cloud account by breaching the provider's security or defenses, they can completely bypass the device's security. If that sounds impossible, consider that Evernote, for example, once had to reset 50 million user passwords after its database was breached.

Even "encrypted" notes aren't secure enough

While some note-taking apps offer encryption, it's typically not as strong as what's found in password managers. For example, Apple's Notes app allows you to lock notes with a passphrase, using end-to-end encryption with AES-GCM.

Not all note-taking apps offer this level of security, however. Evernote's encryption, for example, is more limited: It allows you to encrypt text in your notes using AES-128, but this requires you to do it manually for each sensitive piece of text. More importantly, Evernote's standard storage isn't end-to-end encrypted by default, so the company theoretically has access to your data on its servers. Certainly not the best way to store passwords.

In addition to weak encryption, note-taking apps lack many essential password management features. For example, they lack secure password sharing; automatic password generation to create strong, unique passwords that match a site's specific requirements; and they don't provide breach monitoring alerts to notify users when their stored credentials appear in known data breaches.

Last but not least, they can't autofill login forms on websites, so you have to manually copy your password to the clipboard, and there are quite a few types of malware designed to monitor and steal clipboard contents.

Secure Alternative: Password Manager

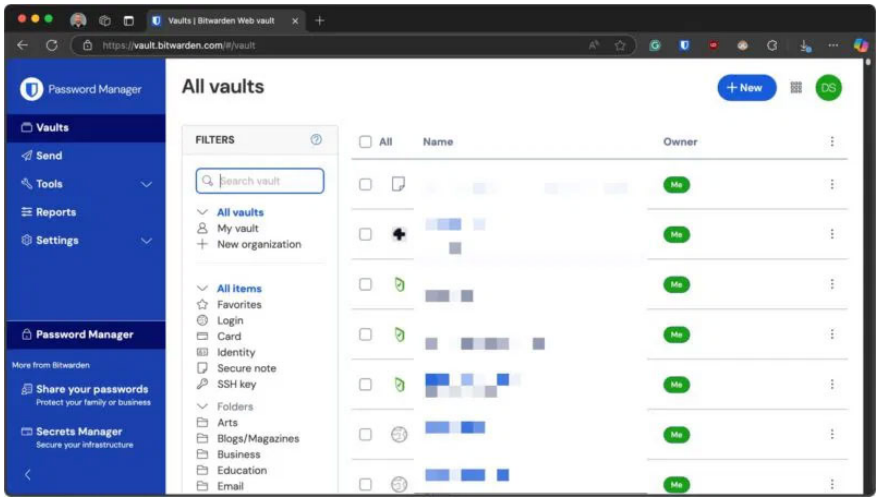
At this point, you might be thinking, 'Okay, if I don't have to use my note-taking app, what's the best way to store my passwords ?' The answer is to turn to a password manager. Password managers are apps specifically designed to securely store your passwords (and other private information). They encrypt everything with a master password (or passphrase) that only you know, and come with convenient features like autofill, strong password generators, and sync across multiple devices.

Here are some of the top password managers that the article recommends, based on different needs and personal experience using them.

1. Bitwarden
2. KeePassXC
3. 1Password

Best Overall: Bitwarden

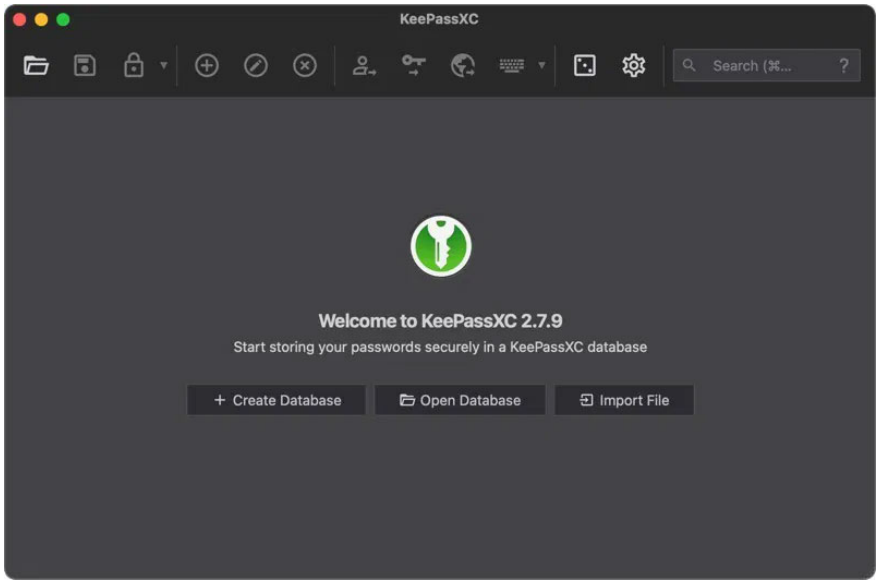
Bitwarden is the top choice for most users. It's free for basic use, open source (meaning its code is public and reviewed by the community), and available on every platform: Web, PC, Mac, Linux, iOS, Android, browser extensions – whatever you want.



Bitwarden strikes the perfect balance between security and usability. Bitwarden has a handy feature called Bitwarden Send that allows you to send encrypted text or files to others. You can use this feature to securely share Wi-Fi passwords and other private information with friends.

Best Local: KeePassXC

Maybe you're someone who doesn't trust cloud services when it comes to passwords. Maybe you're a Linux user or just someone who values ??privacy. In that case, KeePassXC might be the ideal choice.

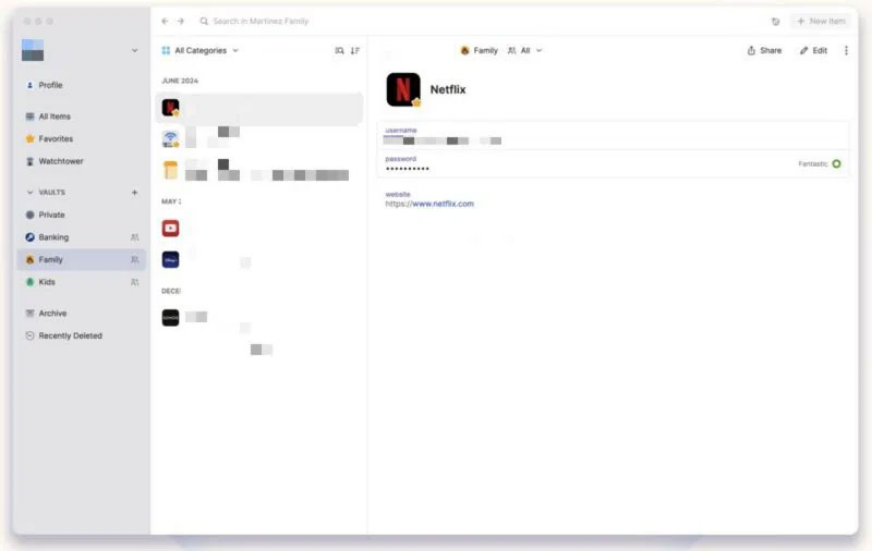


KeePassXC is the community-run successor to the classic KeePass, a respected name in the password management space for years. Unlike Bitwarden, KeePassXC stores everything locally. Your passwords are in an

encrypted database file on your own device. (You can still sync that file via Dropbox or a similar app if you want, but you're still in control.)

Best User Experience: 1Password

1Password is a paid product (there's no free plan, unfortunately), but in return you get a highly rated app that many consider the gold standard for user experience.



The app makes everything easy. The design is clean and friendly, with clear prompts and instructions when setting up. The app is also very integrated. On iPhone and Mac, for example, 1Password feels like a native part of the system (it even works with the Apple Watch to unlock), and on Windows or Android, the app works just as well.

Once you've switched to a password manager and figured out the best way to store your passwords, you can breathe a sigh of relief knowing that an accidental note-taking app sync or device theft won't expose your entire online identity.

Hope you find the right choice!