3 Best Offline Password Managers for MYKI Users

New York City, New York Mar 16, 2022 (Issuewire.com**)** - For many years, MYKI held the reputation as one of the best password managers in the market, but they recently got acquired and will be shutting down operations from April 10th, 2022. Their existing products, such as the MYKI app and extension, MYKI for MSP will cease to exist afterward.

The next step for MYKI users is to seek credible alternatives to move on. Before doing that, you have to consider some of the best features and advantages of MYKI that you enjoy and look for them in these alternative options.

MYKI has several features that make it one of the best password managers available. Some of its best features are:

Offline Password Storage: Unlike many other password management platforms, MYKI stores passwords offline. All the passwords added on this platform are stored locally on your device.

Form Filling: The form-filling feature is in handy. You can not only autofill passwords and other data in any native application or terminal but also autofill credentials into other remote session services.

Two-Factor Authentication: MYKI has a stored two-factor authentication. If you've set up 2FA for your login on any platform, you can add it to MYKI automatically. It also helps to save time as it holds the 2FA for all your logins in one location.

Approve Login: After pairing your app and extension, you need to approve login on your app whenever you want to sign in to an account on your browser.

Password Sharing: With MYKI, you can share passwords with other people securely without revealing your pin and exposing all your information.

In addition to the above, MYKI has many other features, such as Saving Payment Cards, Record Account Histories, Biometric Authentication, Password Generator.

Best MYKI Alternatives

Here are the three best MYKI alternatives. These platforms have many similar features to MYKI, and they also store passwords offline. Read about all three and determine which one best fits you.

1. ID Guard Offline

ID Guard Offline stores your passwords and data totally offline with an excellent security model. It allows you to verify the technologies by yourself, so you don't need to trust anyone. With this app, you don't need to lock your online accounts or struggle with the complicated procedures of resetting passwords. Instead, of allowing it to keep and remember your passwords, you'll remain safe online.

This offline password manager uses a security chip to protect your stored password. It's the same chip used for protecting payment cards in smartphone wallets. Essentially, it completely protects your digital identity and keeps you safe from digital sharing and storage risks. Not only can you access all your passwords from your devices, but this app also ensures that you log in securely into apps and websites with a button click. Also, it is undoubtedly the most optimized platform for importing data from MYKI, including passwords, 2FA, payment cards, ID cards, secure notes, and identities.

Pros

√ Strong encryption & high-level security

√ Numerous verifiable technologies

√ Good import support for MYKI

√ User-friendly interface

Cons

-No data sharing

-No desktop programs

Some of the features and functions of the ID Guard Offline are similar to MYKI's even though they have different architecture and design principles. Essentially, this platform also seems to provide better

security than MYKI, and this is a necessity for the best password management platforms. These are some of the reasons it tops the MYKI alternatives list. It also has a couple of useful additions that make it stand out from the rest:

True Offline (No Cloud Storage)

A prominent feature of this platform is that it's true offline. It offers a high level of privacy protection because it doesn't require internet, signup, or login, and it doesn't collect personal information. Unlike other password managers, it doesn't require any information from you, so it has no idea who you are. Not only does it protect you from hackers, but it also means you don't have to bother with promotional emails or ad tracking.

ID Guard Offline is the complete embodiment of an offline password manager. It stores passwords offline, so all the data stored on your mobile phone is not and cannot be sent to a cloud server secretly. You can also verify this security design by checking the permissions on your android device or app activity on iOS devices.

Security Chip Encrypts Data

Unlike other password managers, it uses a security chip to protect the stored data instead of using a master password. This means that your data safety is no longer reliant on a master password. So, even if hackers get to clone your app to steal your encrypted database or use brute force attacks to steal your master password, they would still be unable to decrypt and view your data. Every time you want to access your passwords, you will receive an automatic prompt to authenticate.

Setting a master password on this platform only acts as another protective layer, and you can send this to your friends in an encrypted format in case you ever forget it. So, your friends can help you save the master password, but it remains encrypted, and they cannot decrypt it or access your database.

Autofill on Desktop Browsers

This platform differentiates the two surfaces susceptible to attack, namely storage and network. It securely stores the passwords offline totally, and the extension uses a remote autofill framework without storing any passwords. As a result, the app can help users fill their data on desktop browsers.

To use this feature, you have to scan the QR code that shows up on a web page with a login form using the ID Guard Offline app. Choose the account, and the login form will be filled in automatically. This feature is similar to MYKI's approving login through its app since they both need the app to autofill on the extension.

Unlike other password manager extensions, ID Guard Offline extension doesn't save your passwords. Instead, the passwords are stored on your phone with sandbox and security chip protection. Passwords cannot be sent to any browser automatically unless you use the app to scan the QR code. This makes it impossible for malicious websites or desktop programs to steal your passwords.

OTP Authenticator (2FA)

This app integrates an OTP authenticator for facilitating 2FA. It's easy to keep OTPs and passwords in one record. And of course, it supports filling OTP on the extension with only one click.

This feature is crucial for MYKI users. And ID Guard Offline supports importing MYKI 2FA, which doesn't happen with many other password managers.

Besides the above, ID Guard Offline also has many other features, such as Advance Phishing Detector, Saving Payment Cards, Timeline, Biometric Authentication, Account Templates, Password Generator.

2. Enpass

Enpass is an offline password manager. The passwords are stored on your device locally and by default, but you have the option of syncing them to a third-party cloud hosting platform such as iCloud, Dropbox, and OneDrive, or sharing with others via Wi-Fi.

It's available for most platforms and offers many features. A paid subscription is optional and it operates differently from many other paid password management platforms. It allows you to store up to 10 credentials for free on your phone, but you'll have to subscribe to the paid version for more space. Enpass also generates secure passwords, stores the passwords, and fills them in automatically on mobile and desktop.

Pros

√ Additional data security by SQLCipher

√ Strong free desktop versions

√ Customizable self-hosting or cloud

√ Plans diversity

Cons

-Unsecured password sharing features

-No multifactor authentication options

Offline Storage and Syncing

Enpass is designed primarily for offline use and it keeps your data only on your device default. It does not save your data on their cloud server. But you are allowed to sync them to a third-party cloud hosting platform. In the settings of the Enpass app, you can choose to sync your data to lots of cloud services including Dropbox, iCloud, Google Drive, One Drive, WebDAV, Box, Nextcloud, Wi-Fi Sync.

Like ID Guard Offline, Enpass does not ask you to sign up with any phone number or email address. After downloading the app, you just need to set a master password to use it. Not submitting personal information helps protect your privacy.

Secure Encryption with AES-256

The Enpass server is encrypted with the AES-256 military-grade cipher as other password managers to safeguard your data on your device or in a third-party cloud server. It also uses the open-source encryption engine SQLCipher to help strengthen the encryption. The key that encrypts your data is

derived from the master password you set. So please do set a strong one.

There is no record of your master password or its derivative with Enpass. And unlike ID Guard Offline, Enpass does not have the Find Back Master Password feature. If you forget your master password, there is no way to recover your data. That means, all your data will be lost. So please do remember your master password.

Desktop App and Extension

Enpass offers apps and extensions on desktops. Unlike other password managers, Enpass only allows you to use the extension with the help of the desktop app. Enpass Browser extensions work in conjunction with the desktop application for auto-filling usernames, passwords, credit cards, and identities on the web pages. It also lets you generate strong & unique passwords, saves new logins to avoid the copy/paste details between the main app and browser, and a lot more.

The service is available for free if you're content with using the desktop version alone. However, if you need to switch between mobile accounts and desktop versions, you need to pay. The mobile version is paid-only, so you can either subscribe to this service or pay as a one-time user. Then you can reactivate your subscription through the desktop or mobile app at any time.

Autofill and OTP Authenticator

Like MYKI, Enpass allows you to autofill passwords, logins, credit cards, and other information on apps or websites. You can also use it to save OTP for other platforms.

Besides the above, Enpass also has many other features, such as Smartwatch Support, Biometric Authentication, Saving Payment Cards, Password Generator.

3. KeePass

KeePass is also among the best password managers that store data offline. It is a potent and customizable tool, and it's completely free. The only thing is that you're responsible for putting most of the pieces together. At the core, the KeePass desktop application was created for Windows and required some tweaking before it works on Linux or Mac.

Your files can be shared to your local home network or on the cloud, with accounts such as OneDrive, Dropbox, or other similar accounts. You also have to choose from the numerous third-party apps for iOS, Chrome OS, Android, other platforms, and third-party browser extensions. This is easy because of the hundreds of extensions and plugins that work seamlessly with KeePass.

Pros

√ Open-source

√ Completely free

√ Various clients available

√ Lots of customization

Cons

-Outdated and unfriendly UI

-No customer support

Offline and Free

KeePass stores the data locally on your device. If you prefer to send your data to cloud storage, though, you're free to use that as a backup. You can put the KeePass credentials database on cloud-syncing folders, like OneDrive, Google Drive, etc.

KeePass is an open-source tool and everyone can check its codes. Most importantly, it's completely free. However, it has an outdated and unfriendly UI and may be a little bit difficult for average users to use. And It may be a little cumbersome to set up this platform on multiple devices.

Secure Encryption

KeePass employs the AES-256 or SHA-256 encryption standard to protect your data. Like Enpass, the key that KeePass used to encrypt your data is derived from the master password you set. So do set a strong one.

You can also use the key file to help create 2FA protection. But pay attention to the reminder from KeePass official: The point of a key file is that you have something to authenticate with (in contrast to master passwords, where you know something), for example, a file on a USB stick. The key file content (i.e. the key data contained within the key file) needs to be kept secret. The point is not to keep the location of the key file secret - selecting a file out of thousands existing on your hard disk basically doesn't increase security at all, because it's very easy for malware/attackers to find out the correct file (for example by observing the last access times of files, the recently used files list of Windows, malware scanner logs, etc.). Trying to keep the key file location secret is security by obscurity, i.e. not really effective.

Cross-platform Support

KeePass officially only provides desktop apps. If you want to use it on Android and iOS, you have to use third-party tools, like KeePassDroid (for Android), KeePass2Android (for Android), Strongbox (for iPhone / iPad / MacOS).

KeePass also has many features, such as Autofill, Password Generator, Password Groups. However, it's more recommended to technical users. If you don't want to spend time learning it, you'd better choose ID Guard Offline or Enpass. These two are easier to use.

Conclusion

As an MYKI user, you have less than a month to transfer your data before it shuts down. So you're probably looking for other offline password managers that can serve as alternatives. This article discusses three excellent MYKI alternatives, but the top pick is ID Guard Offline because it is the most optimized to import files from MYKI, and it has almost all the features that MYKI has. It also has a great security model, which makes it even more ideal for you if you attach great importance to security. You may also decide to download all three so you can try them out and determine the best one for you.

Media Contact

Blue Space Information Technology Co.,Ltd

contact@bluespace.tech

Source : Blue Space Information Technology Co.,Ltd

See on IssueWire