Review: Myki password manager.

Last Revised 07 July 2018.

Contents of this article.

1. Introduction.

Managing multiple accounts across various platforms leads to the challenge of storing numerous passwords, causing significant frustration. Consequently, numerous password management services have emerged. Traditional password managers typically require online login to select and use a secret. However, Myki takes a unique approach by storing secrets directly on your phone, offering an added layer of security and convenience.

2. What is Myki?

Myki functions as an authenticator and password manager through its mobile app and compatible browser extension for Chrome, Opera, Safari, and Mozilla Firefox. To pair the app with the browser, users must scan a QR code. What distinguishes Myki from other password managers and authenticators is its unique approach: passwords are not stored on external servers or in the cloud; instead, they reside solely on your mobile device for added security.

Website: https://myki.co/

3. Pros.

- Myki's interface is user-friendly and straightforward.
- Pair passwords with different computers via fingerprint or PIN code authentication.
- Myki refrains from storing browsing data, mouse, or keystroke logs (Testing Criteria: Zero-knowledge).
- Passwords are solely stored on your phone without any cloud backup (Testing Criteria: Zero-knowledge).
- Encryption secures all traffic between your phone, Myki servers, and browser extensions (Testing Criteria: End-to-end encryption and implementation).
- AES-256 encryption protects passwords exchanged between the phone and browser extension via QR code scan (Testing Criteria: End-to-end encryption and implementation).
- Public key cryptography authenticates users; the server verifies signed challenges unlocked by pin codes or fingerprint sensors (Testing Criteria: End-to-end encryption and implementation).
- Remote logout from computer accounts is possible through Myki's mobile app.
- Myki stores and auto-fills two-factor authentication tokens.
- In case of a data breach, Myki's lack of sensitive data storage prevents forced access (Testing Criteria: Zero-knowledge).
- No master passwords or passphrases are necessary.
- Unlimited pairing and login across various computers.
- Available on multiple devices - tablets, desktops, laptops (browser extensions), Android, and iOS (Testing Criteria: Multiplatform).
- Responsive customer support provided by Myki.
- Supports credit card integration for online autofill similar to password autofill.

• Encrypted password sharing among Myki users via peer-to-peer connection without revealing passwords (Testing Criteria: Zero-knowledge).

• Revocable access to shared passwords.

• App prevents screenshots during use.

• Chrome extension features a password creator for intricate and secure password generation.

• Multiple team accounts managed on one device with distinct permissions for agents, admins, departments, friends, or family, priced per user count within each team.

4. Cons.

• Myki app inserts passwords into pages, potentially exposed to hacking or inspection by hackers, state-sponsored criminals, or knowledgeable users intercepting JavaScript execution for password retrieval.

• Myki entails a high cost for usage.

• Certain features are incompatible with older Android versions, such as the absence of the location feature in Android 6.0 Lollipop.

• Screen recording applications pose a risk of capturing passwords or actions while using Myki.

• Myki lacks open-source accessibility (Testing Criteria: open-source).

• Slow internet connections sometimes prevent saving newly created secrets from the dashboard.

• Unencrypted URLs are utilized for website icon retrieval, raising concerns about potential tracking activities.

5. Conclusion.

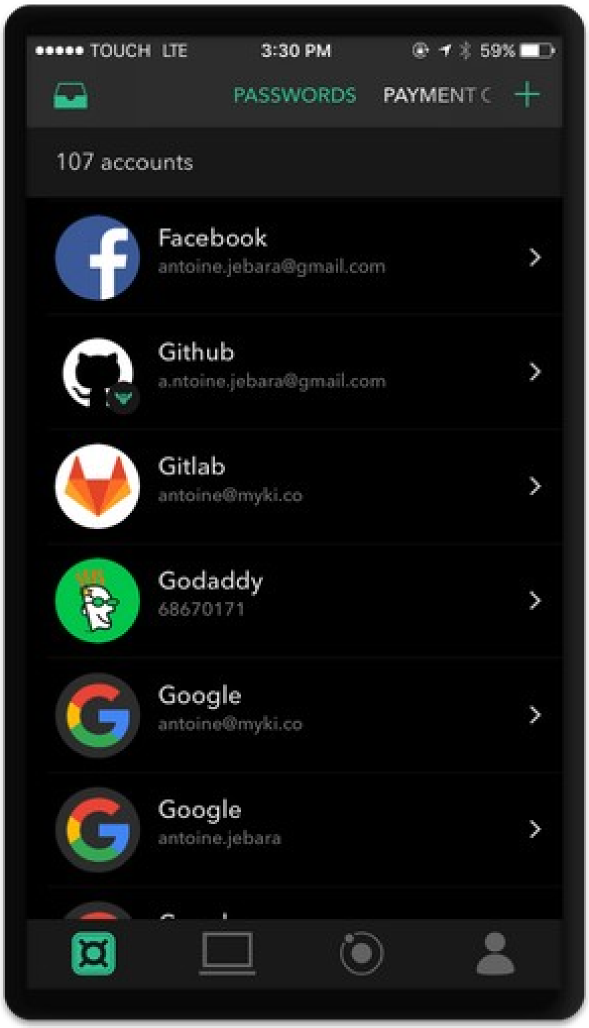
Myki effectively achieves its primary objective of ensuring passwords maintain a high level of complexity, making them challenging to decode, decrypt, hack, or access. The password manager's notable feature is its use of the phone to store passwords, providing assurance that sensitive information is not stored in the cloud or on remote servers vulnerable to breaches. This unique approach puts control directly in the user's hands.

Passwords can be easily viewed within the app, and users have the option to disable access even without physical contact with the phone. In the event of a lost or stolen phone, users can promptly revoke access to the device. However, a drawback is the lack of access to Myki's source code for independent review, as it is not open source.

Myki also monitors various parameters such as physical addresses, IP addresses, geographic locations, login data, and battery levels through the administrative panel. This helps identify unusual activities or irregular behavior within the app. In the event of a potential hack, whether initiated by the user or external threats, Myki's administrators can swiftly perform a mass reset, issuing new passwords to all users. The app's responsive support staff promptly addresses reported bugs, further enhancing its reliability.

In conclusion, Myki receives high ratings and proves to be a suitable choice for both individuals and organizations.

6. Screenshots.



107 accounts

Facebook
antoine.jebara@gmail.com

Github
a.ntoine.jebara@gmail.com

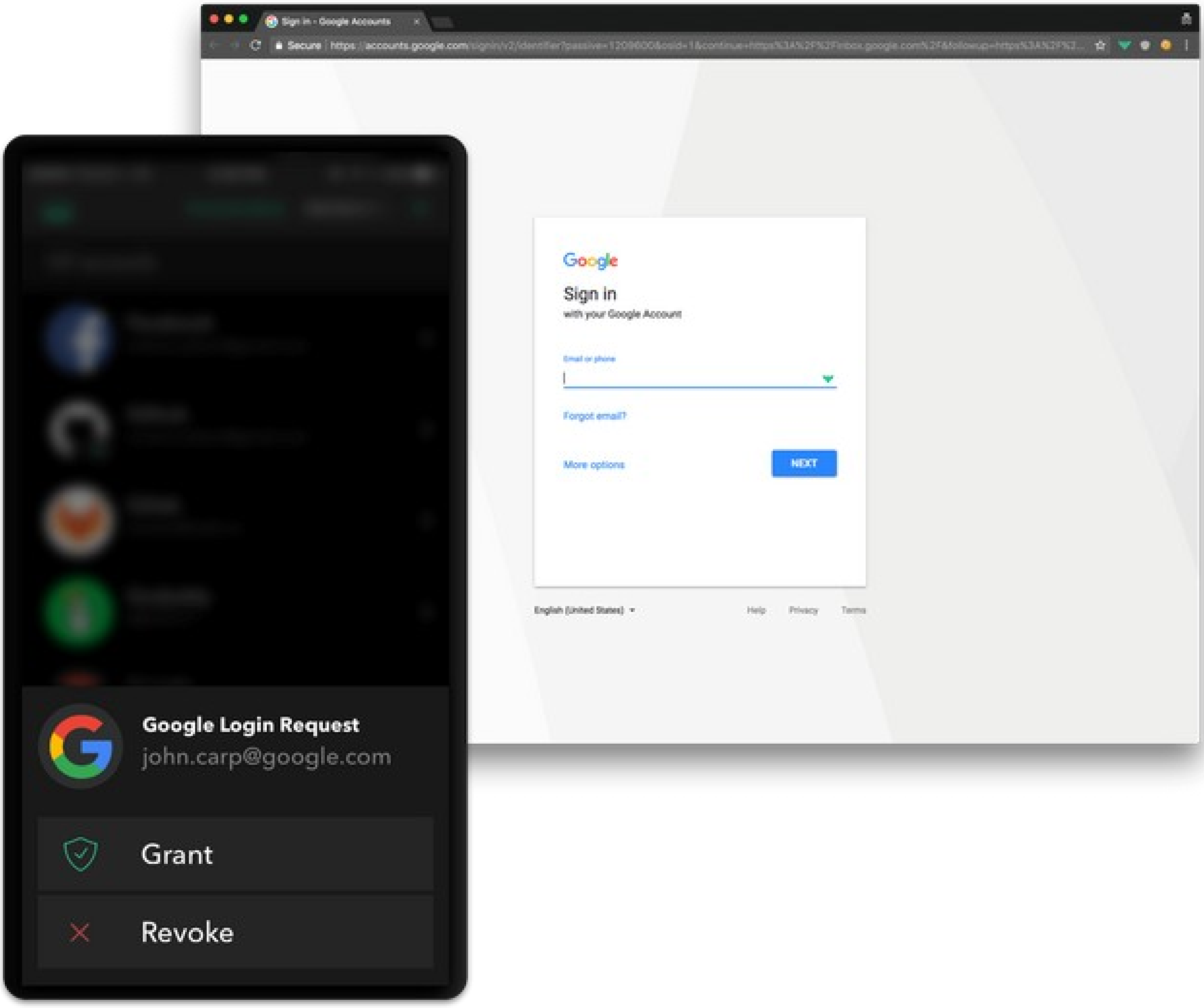
Gitlab
antoine@myki.co

Godaddy
68670171

Google
antoine@myki.co

Google
antoine.jebara

Screenshot 1: Myki UI.



Google

Sign in

with your Google Account

Email or phone

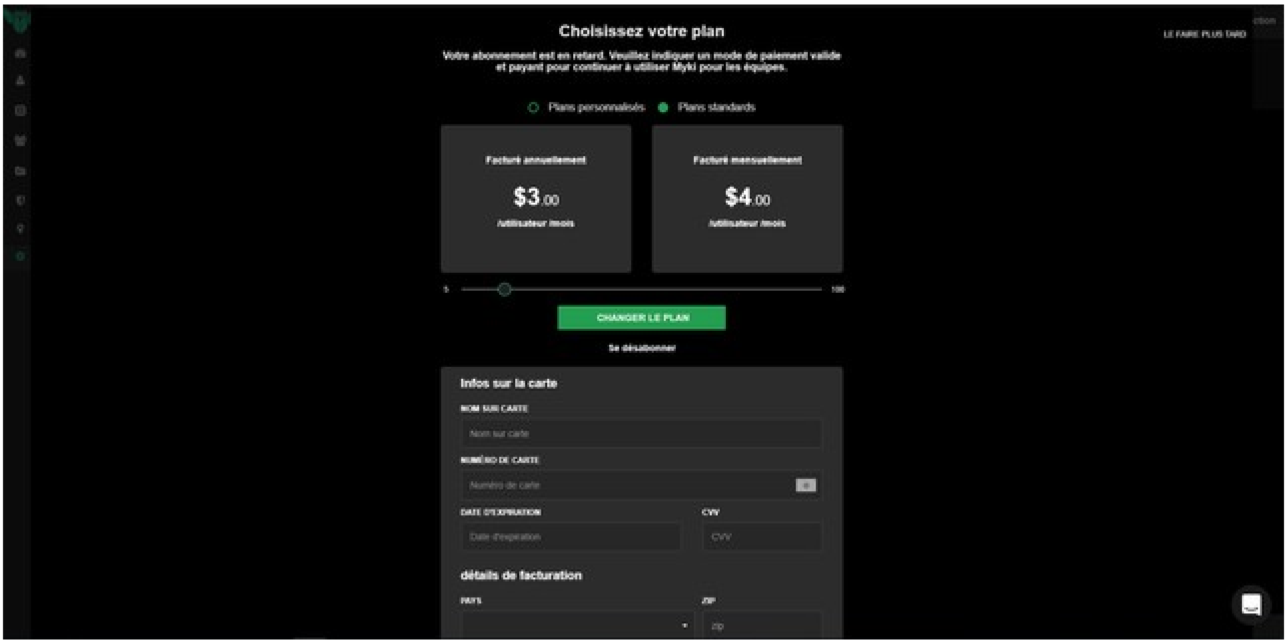
Forgot email?

More options

Google Login Request

john.carp@google.com

Screenshot 2: Secret login request.



Choisissez votre plan

Votre abonnement est en retard. Veuillez indiquer un mode de paiement valide et payant pour continuer à utiliser Myki pour les équipes.

○ Plans personnalisés ● Plans standards

Facturé annuellement	Facturé mensuellement
$3.00	$4.00
/utilisateur /mois	/utilisateur /mois

Infos sur la carte

NOM SUR CARTE: Nom sur carte

NUMÉRO DE CARTE: Numéro de carte

DATE D'EXPIRATION: Date d'expiration

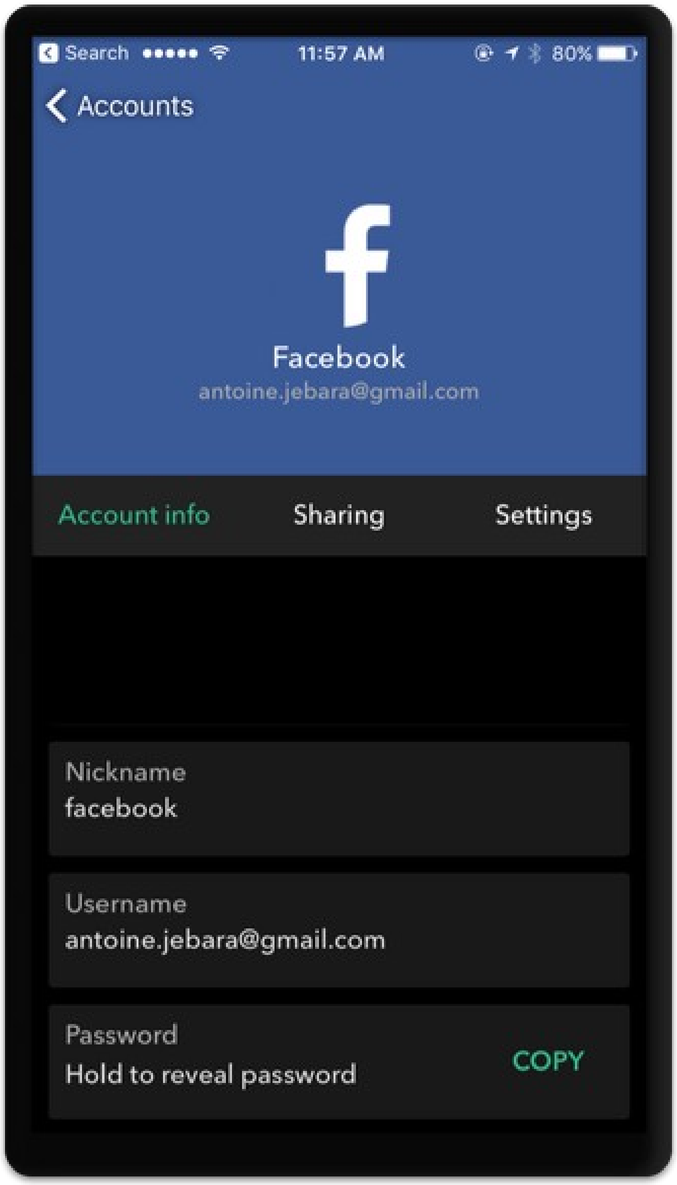
CVV: CVV

détails de facturation

PAYS:

ZIP: zip

Screenshot 3: Sharing center.



Facebook
antoine.jebara@gmail.com

Nickname
facebook

Username
antoine.jebara@gmail.com

Password
Hold to reveal password

Screenshot 4: Example of a secret.

7. Criteria used for testing:

- **Zero-knowledge:** Currently, Myki doesn't maintain complete zero-knowledge functionality. It retains metadata like auto-generated unique IDs for stored accounts, phone numbers for recovery, and shared account IDs for access revocation. However, Myki does not log browsing data, mouse movements, or keystrokes.

- **End-to-end-encryption and implementation:** Myki ensures robust end-to-end encryption by employing the AES256-CBC encryption algorithm, recognized as one of the most secure standards. This algorithm guarantees the safety of your data during transfers. The encryption key is shared exclusively between your mobile device and the browser extension via a QR code scanned through the Myki app's camera, ensuring that none of your encryption keys are transmitted over the web. The AES key, generated by your browser extension, establishes a visual connection with Myki. This method stands as a highly secure means to safeguard encryption keys.

• **Open-source:** Myki's lack of open-source accessibility stands as a significant drawback, limiting the ability to review or verify the contents of its source code.

• **Multiplatform:** Myki is accessible on mobile platforms, including iOS and Android. On desktops, it functions as an extension compatible with Google Chrome, Firefox, Safari, and Opera.

• **Resistance to state-sponsored criminals:** Individuals such as police officers and prosecutors, among others, pose a unique threat as their actions are often deemed legal due to corruption within state institutions, making them formidable criminals on both individual and national levels. Their ability to cover up illegal activities is concerning; they can intercept and read IMAP, POP3, TLS, and SSL communications. Additionally, they can spoof email provider SSL certificates and access SMS and emails, making recovery options vulnerable to exploitation. Therefore, it's crucial to utilize encryption software, encrypt devices, and consider purchasing hardware from locations outside the operational country.

8. Sources.

Myki For Teams - Product Hunt. (2018). Retrieved from: https://www.producthunt.com/posts/myki-for-teams

Myki rolls out a password manager that locks all your info away on your phone. (2018). Retrieved from: https://techcrunch.com/2016/09/13/myki-rolls-out-a-password-manager-that-locks-all-your-info-away-on-your-phone/

Password Fish - Product Hunt. (2018). Retrieved from: https://www.producthunt.com/posts/password-fish

Secure Offline Storage - Myki Password Manager. (2018). Retrieved from: https://myki.co/features/offline-storage

Solution, H. (2018). How Myki, with its cloudless solution, plans to be the death of the password. Retrieved from: https://yourstory.com/2017/10/app-fridays-myki-death-to-passwords/