UBINODES

REVIEW:

MYKI PASSWORD MANAGER

Contents of this article.

1. Introduction.

Managing multiple accounts across various platforms can be frustrating due to the need to store numerous passwords. This has led to the emergence of many password management services. Traditional password managers typically require an online login to access and use your passwords. However, Myki offers a unique approach by storing passwords directly on your phone, providing an added layer of security and convenience.

2. What is Myki?

Myki functions as both an authenticator and a password manager through its mobile app and compatible browser extensions for Chrome, Opera, Safari, and Mozilla Firefox. To pair the app with the browser, users must scan a QR code. What sets Myki apart 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 enhanced 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 Security Concerns: The Myki app inserts passwords into web pages, which could be exposed to hacking or inspection. This vulnerability arises from the possibility of hackers, state-sponsored criminals, or knowledgeable users intercepting JavaScript execution to retrieve passwords.

• 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 used for retrieving website icons, which raises concerns about potential tracking activities.

5. Conclusion.

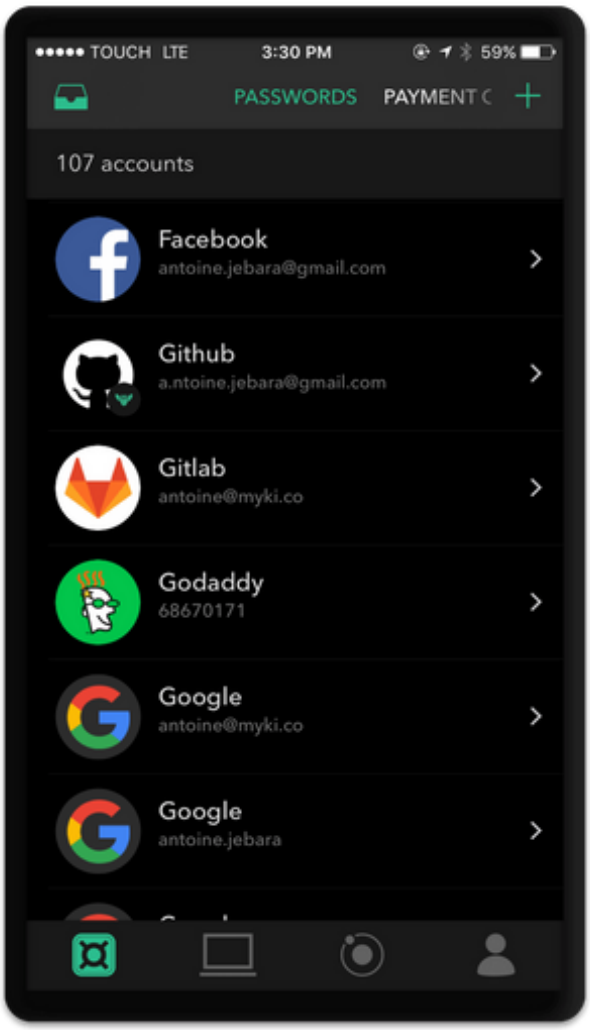
Myki effectively achieves its primary objective of ensuring passwords remain highly complex, making them difficult to decode, decrypt, hack, or access. A key feature of this password manager is its use of the phone to store passwords, ensuring that sensitive information is not stored in the cloud or on remote servers, which could be 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 that Myki's source code is not open source, meaning it cannot be independently reviewed.

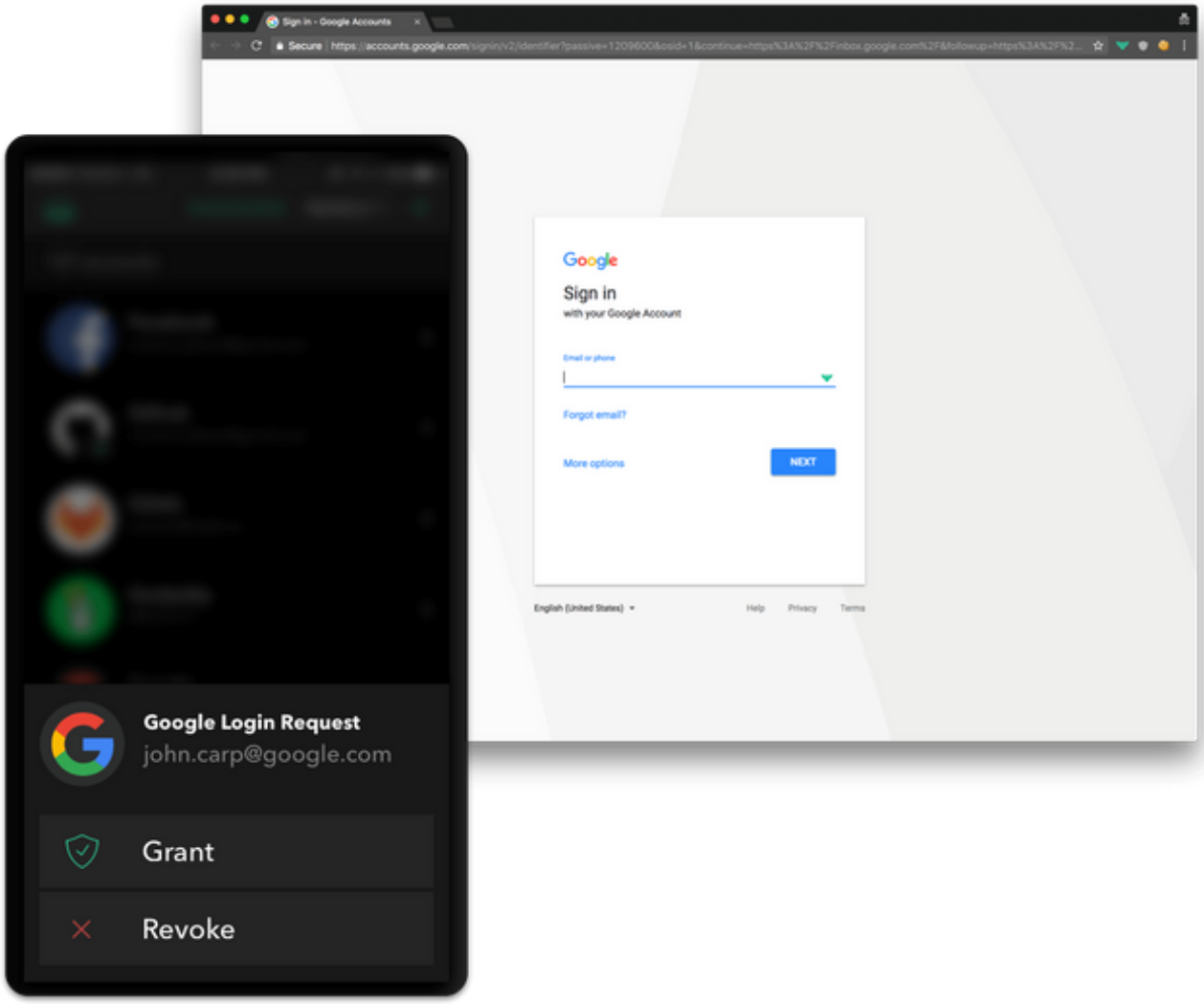
Myki also monitors various parameters such as physical addresses, IP addresses, geographic locations, login data, and battery levels through the administrative panel. This helps identify unusual activities or irregular behavior within the app. In the event of a potential hack, whether initiated by the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

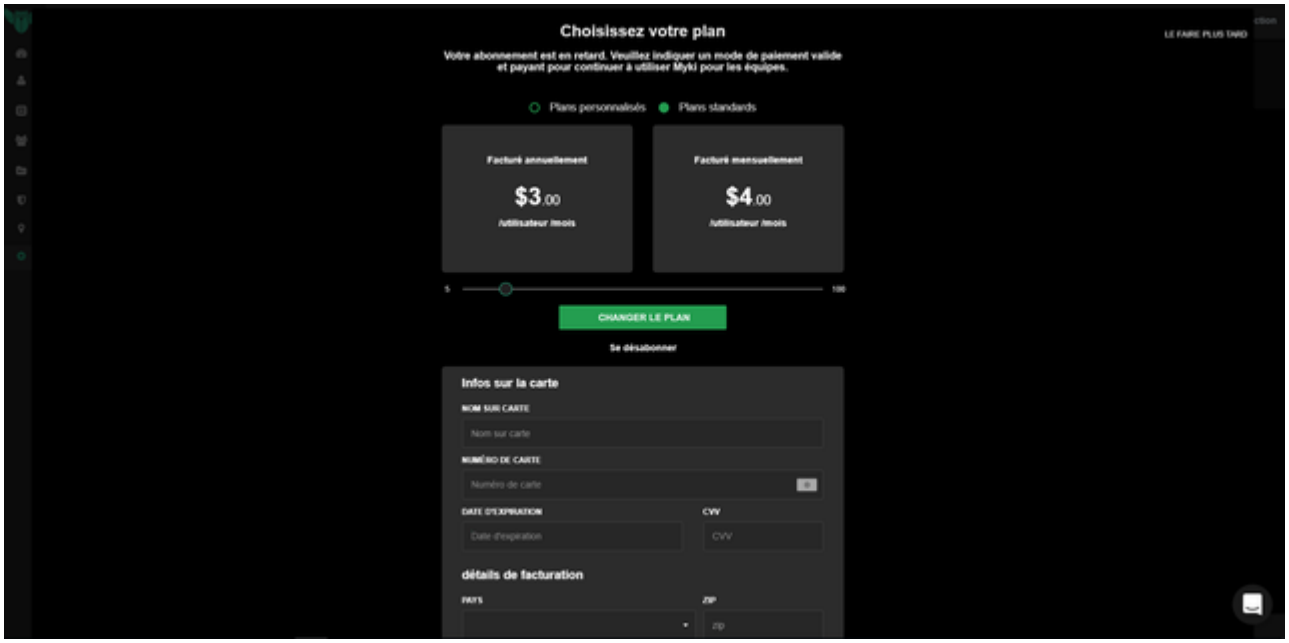
6. Screenshots.



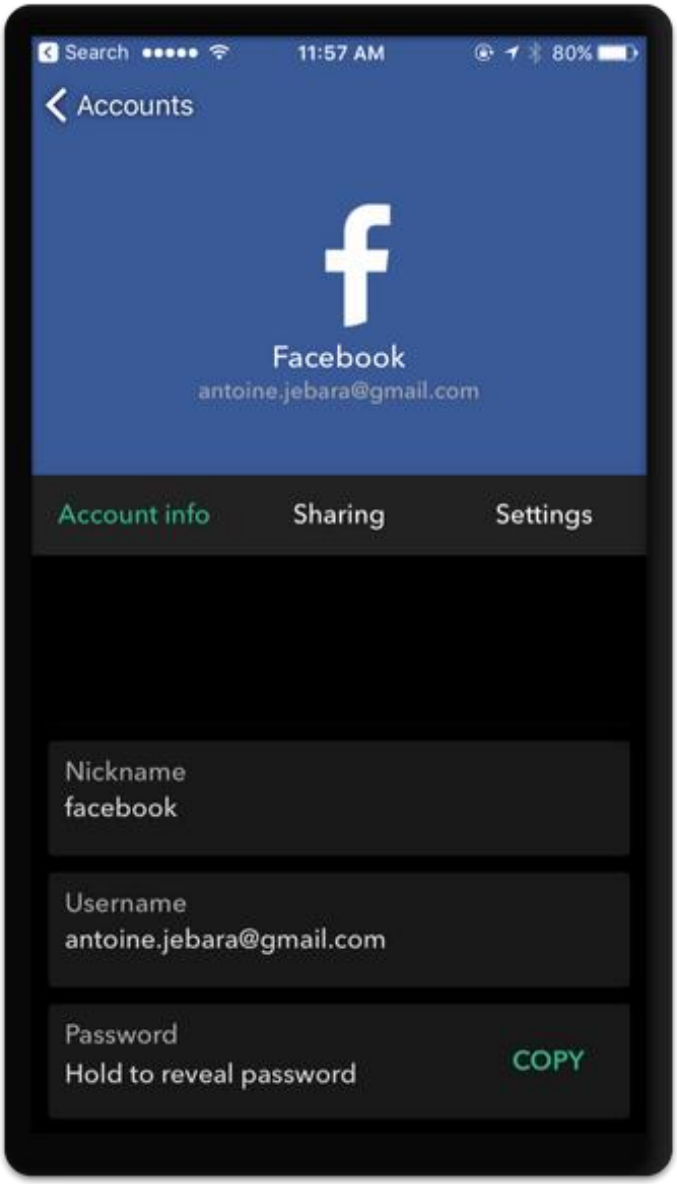
Screenshot 1: Myki UI.



Screenshot 2: Secret login request.



Screenshot 3: Sharing center.



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 such as 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 keeps your data super safe by using a top-notch encryption method called AES256-CBC. This ensures that your information stays secure when it's being sent around. The key to this encryption is shared only between your phone and the browser extension through a QR code scan. This means your keys never travel over the internet. The browser extension generates an AES key, which visually connects to Myki for added security.

• **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 works on mobile devices like iPhones and Android phones. On computers, it's available as an extension that works with web browsers like Google Chrome, Firefox, Safari, and Opera.

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

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/

