How Google and Apple's Free Password Managers Compare With 1Password, Dashlane and Others; Free password managers built into popular browsers may work for some, including kids and less tech-savvy loved ones, but they come with some downsides—mainly, where you can or can't use them

Nguyen, Nicole . Wall Street Journal (Online) ; New York, N.Y. [New York, N.Y]11 July 2021.

ProQuest document link

FULL TEXT

With ransomware attacks on the rise—and compromised passwords to blame for some of the hackings—there's no better time to review your personal security practices.

It all starts with how you create and store passwords.

You may have read a thing or two about password managers, perhaps in my previous column on the subject.

This software can create strong randomized passwords, then remember them for you, and they can auto-fill credentials, simplifying the login process. Having unique passwords is critical to your online security: Around 25% of security breaches in 2020 involved the use of stolen usernames and passwords, according to a Verizon report published in May.

In this column, I'm comparing the two main types:

* The free manager built into your web browser or mobile operating system, such as Apple's iCloud Keychain, Google's Password Manager and Firefox's Lockwise.

* Third-party, stand-alone apps that work across multiple platforms; these include Dashlane, 1Password and LastPass.

Keep in mind that there is large variation in usability, security and accessibility among these offerings. For example, Firefox's browser-based Lockwise also has a mobile app that works with both Android and iOS devices, while Google's Password Manager supports Android mobile apps, but not iOS apps. In a move to add an extra bit of protection, 1Password uniquely requires a 64-character "secret key"—in addition to a master password and multifactor authentication—to authorize new devices or web logins.

In June, Tavis Ormandy, a vulnerability researcher at Google, posted an argument against third-party password managers and concluded that the manager built into your browser—like the one Mr. Ormandy's employer itself provides for Chrome users—is best. This took me by surprise. Most security professionals I've spoken to over the years recommend third-party managers because of their ability to work across devices and operating systems.

The problem? Many stand-alone managers rely on browser extensions to auto-fill passwords and other data, and these extensions could be potentially tricked, Mr. Ormandy wrote in his post. In an extreme case, a malicious website could view credentials from unrelated sites, which was the case of a 2017 flaw in the Keeper browser extension on Windows computers . (Keeper issued a fix within 24 hours.)

In 2017, Mr. Ormandy discovered an exploitable vulnerability in LastPass where such an attack could retrieve account information. The company resolved the issue days later. In 2019, LastPass patched another flaw that could expose the last filled credentials. LogMeIn, the LastPass parent company, declined to comment. Mr. Ormandy didn't respond to multiple requests for comment.

"Mr. Ormandy raises some excellent points at a technical level, some of which apply to 1Password," said Rick van Galen, a security engineer with 1Password. "Making secrets accessible across all these platforms can be a scary prospect from a security perspective. That's something we know. We work hard to do this in a way that is secure."

In 2016, 1Password patched a flaw, discovered by Mr. Ormandy, that affected Windows machines. Jeffrey Goldberg, 1Password's director of security, said browsers and operating systems are now better at safely allowing extensions to fill login fields, making it more difficult for malicious websites to trick password managers.

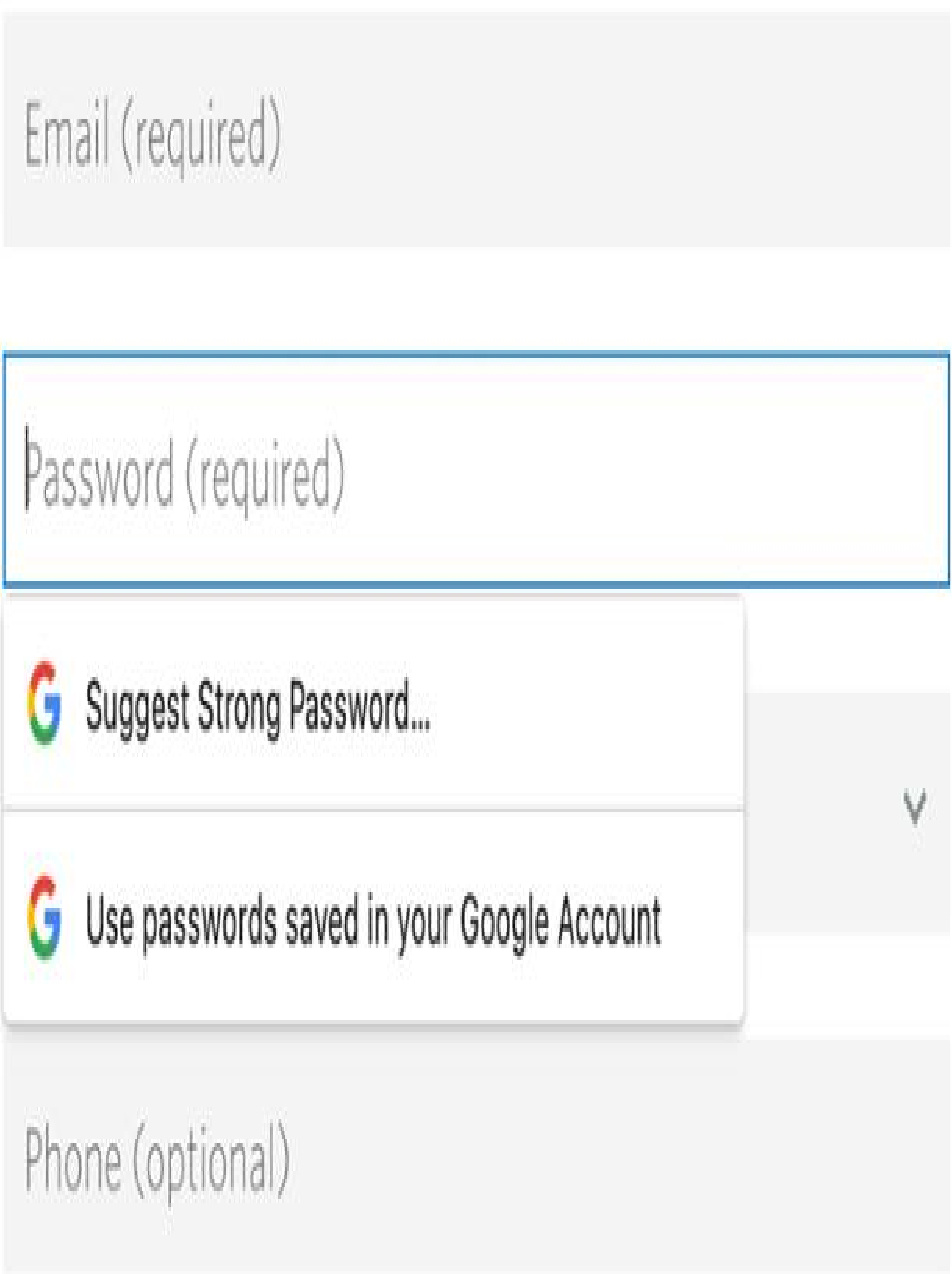
In a published response to Mr. Ormandy's post, Dashlane Chief Technology Officer Frederic Rivain said, "No one can ensure zero risk. What matters from our perspective is that we rely on best practices of the industry to minimize the risk." The company has already addressed some of Mr. Ormandy's outlined issues, he said but didn't detail which.

Also, password-manager extensions work differently on different browsers. Stuart Schechter, a security lecturer at University of California, Berkeley, School of Information, points out that Apple provides a safe space for third-party password managers to transmit credentials securely on iOS devices and Macs. Websites can't interfere with extensions within this framework. Google's Chrome browser doesn't offer this same kind of protection, he said.

"We're always looking for ways to work with extension developers to create solutions that work for them while improving security for users," a Google spokeswoman said.

Dr. Schechter uses browser-based password managers, as recommended by Mr. Ormandy, but said even browser-based password systems aren't perfect.

"If you're a Chrome user, using Chrome's password manager has its own risks. Your passwords are only as safe and accessible as your Google account," he said.



Email (required)

Password (required)

Suggest Strong Password...

Use passwords saved in your Google Account

Phone (optional)

Enlarge this image.

One benefit of built-in password managers is that they're free and easy to use. The caveat? Google's, shown here, only works with Chrome browsers and Android devices. PHOTO: Nicole Nguyen/The Wall Street Journal

And they tend not to store all the different types of login data needed these days: not just usernames and passwords, but PIN codes inside of those apps, answers to security questions and more.

"A browser password manager is better than no password manager at all, but it's just not robust enough to help people manage the overwhelming number of credentials and secrets that come with our increasingly online world," said Jessy Irwin, a security consultant and former head of security at blockchain software company Tendermint. Third-party password managers are better equipped, she said.

So, what does it all mean? While anything is better than reusing the same passwords over and over again, the security of your password manager depends on a variety of factors, including which platform you're using. Here are the pros and cons of each approach, laid out to help you choose what will best fit your life.

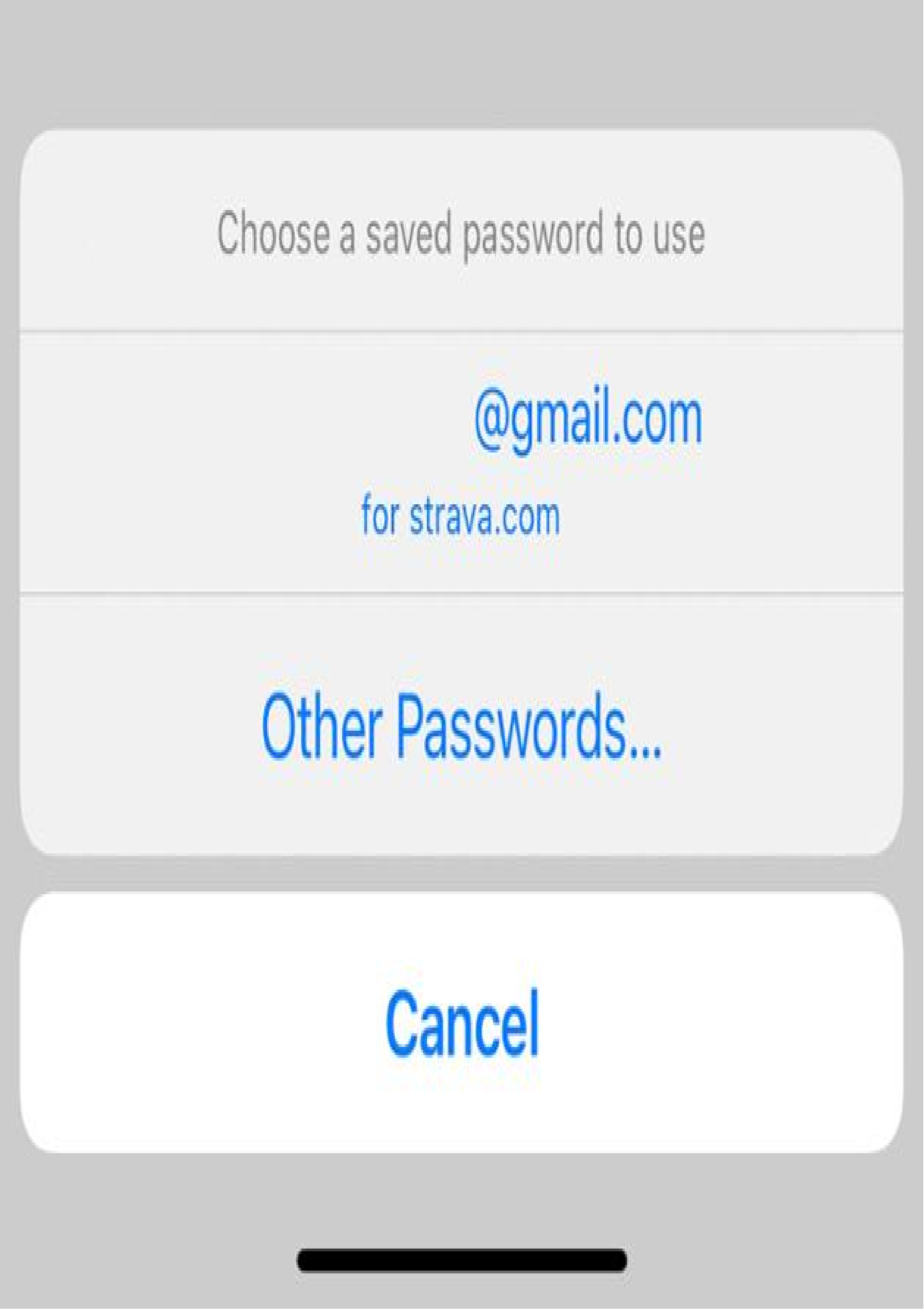
Built-in Password Manager Pros...

If you use the same browser on all platforms, they can work. If you remain within a specific ecosystem (e.g., Google's or Apple's), the built-in manager could meet your needs. If, for example, you use Chrome on your computer and phone, your Google-stored passwords will be accessible on any webpage and—if you use Android—your mobile apps, too. Apple's iCloud Keychain works seamlessly within Apple's walled garden, and even a bit beyond: There's an iCloud Passwords browser extension for Chrome on Windows machines. However, it doesn't support Android devices.

They're easy to use and free. You don't have to download anything, or pay a monthly subscription fee. It might be the best option for kids or non-computer-savvy loved ones to improve their password security.

...and Cons

You can't easily share passwords with others. Google's Password Manager doesn't have sharing capabilities, and Apple's iCloud Keychain only allows sharing with nearby contacts via AirD1Passrop .



Choose a saved password to use

@gmail.com

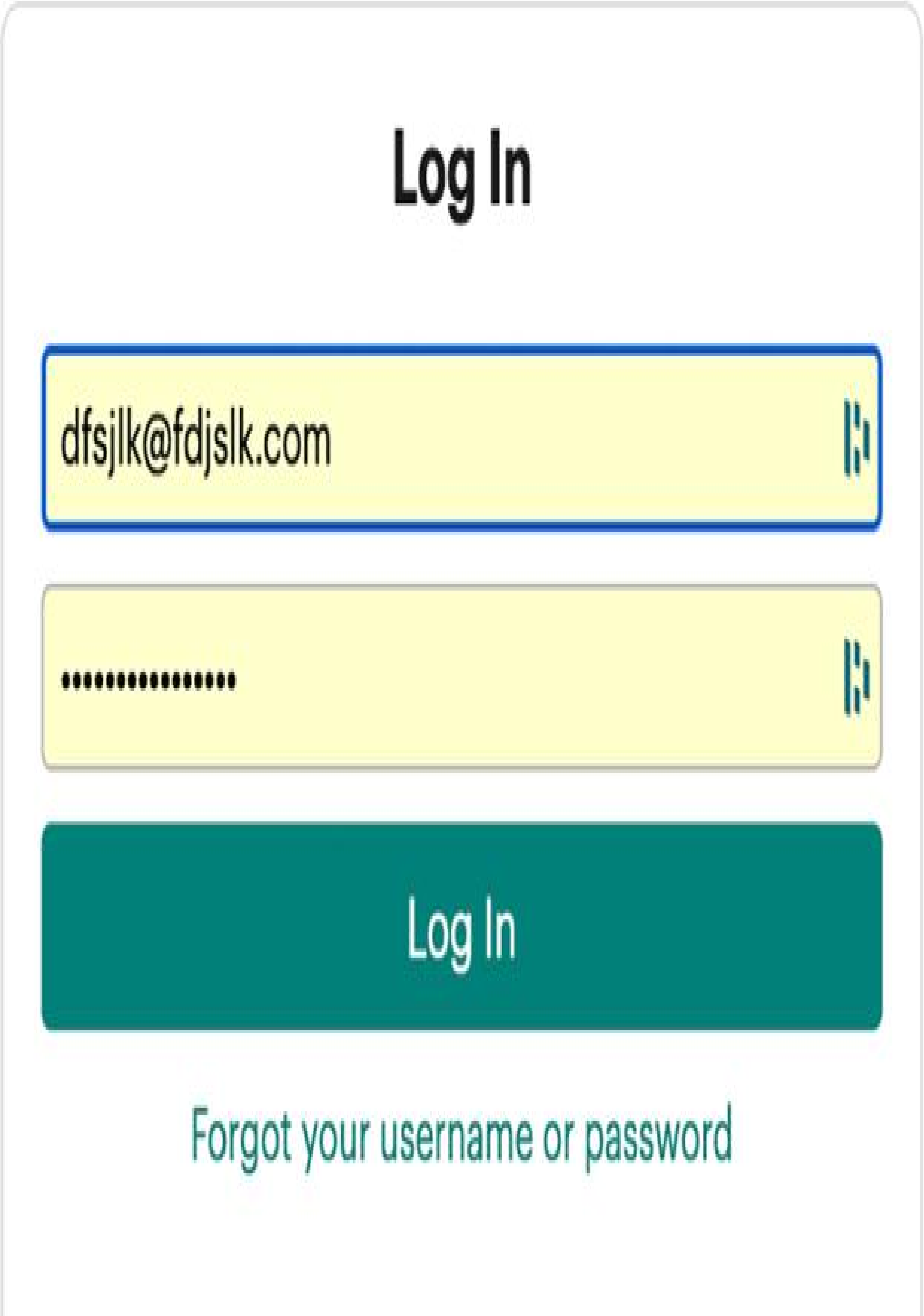
for strava.com

Enlarge this image.

iCloud Keychain is the password system for iOS and Mac devices. Apple also offers an extension, iCloud Passwords, that works with Chrome on Windows. PHOTO: Nicole Nguyen/The Wall Street Journal

Apple's iCloud Keychain is tough to leave. If you want to switch to another password manager, Google makes it relatively easy for you to export passwords , but Apple doesn't provide a similar password export option.

On Chrome, access to your device means access to your passwords. Google's Password Manager can't be "locked" and doesn't require a unique master password to auto-fill credentials. However, to view passwords in plain text, you will need to enter your computer password. So make sure the password on your computer or mobile device can't easily be guessed . (Apple's iCloud Keychain requires authentication before auto-filling passwords.)



Log In

dfsjlk@fdjslk.com

••••••••••••••••

Enlarge this image.

In Google Chrome, browser extensions display icons next to login fields, like Dashlane's 'D' shown here, to indicate there is a saved password. PHOTO: Nicole Nguyen/The Wall Street Journal

Third-Party Password Manager Pros...

They're compatible with many different platforms. Most third-party applications—the best being 1Password, Dashlane and LastPass —work with a variety of devices and operating systems. From web apps to smartwatches, you can access passwords from virtually any platform.

You can save different kinds of secrets. Many services include secure, encrypted notes to protect PINs or other kinds of login info, plus credit cards, addresses and more.

There are more granular security settings. For example, you can tell the application to log you out or clear your clipboard after certain periods.

...and Cons

You have to remember your master password. This long string essentially holds the key to your online kingdom, and secure systems don't offer a way to easily recover this master password if you forget. (Dashlane does allow users to set an emergency contact who can help recover your account.) Most managers offer added protection in the form of two-factor authentication, plus extra verification when you log in from a new device or location.

You have to pay for full functionality. Most services—with the exception of the free Bitwarden —require a paid subscription to use the password manager across multiple devices. 1Password doesn't offer a free tier at all. I agree, the growing number of online subscriptions is getting out of hand , but for something as important as passwords, it's probably worth paying for someone to help you guard your digital secrets.

For more WSJ Technology analysis, reviews, advice and headlines, sign up for our weekly newsletter.

Write to Nicole Nguyen at nicole.nguyen@wsj.com

How Google and Apple's Free Password Managers Compare With 1Password, Dashlane and Others

Credit: By Nicole Nguyen

DETAILS

Subject:	Operating systems; Software; Subscriptions; Third party; Security management; Passwords
Company / organization:	Name: Wall Street Journal; NAICS: 511110, 519130
Publication title:	Wall Street Journal (Online); New York, N.Y.
Publication year:	2021
Publication date:	Jul 11, 2021
column:	Personal Technology: Nicole Nguyen
Section:	Tech
Publisher:	Dow Jones &Company Inc
Place of publication:	New York, N.Y.
Country of publication:	United States, New York, N.Y.
Publication subject:	Business And Economics
e-ISSN:	25749579

Source type:	Newspapers
Language of publication:	English
Document type:	News
ProQuest document ID:	2550054309
Document URL:	https://www.proquest.com/newspapers/how-google-apples-free-password-managers-compare/docview/2550054309/se-2?accountid=30665
Copyright:	Copyright 2021 Dow Jones &Company, Inc. All Rights Reserved.
Last updated:	2021-07-11
Database:	The Wall Street Journal