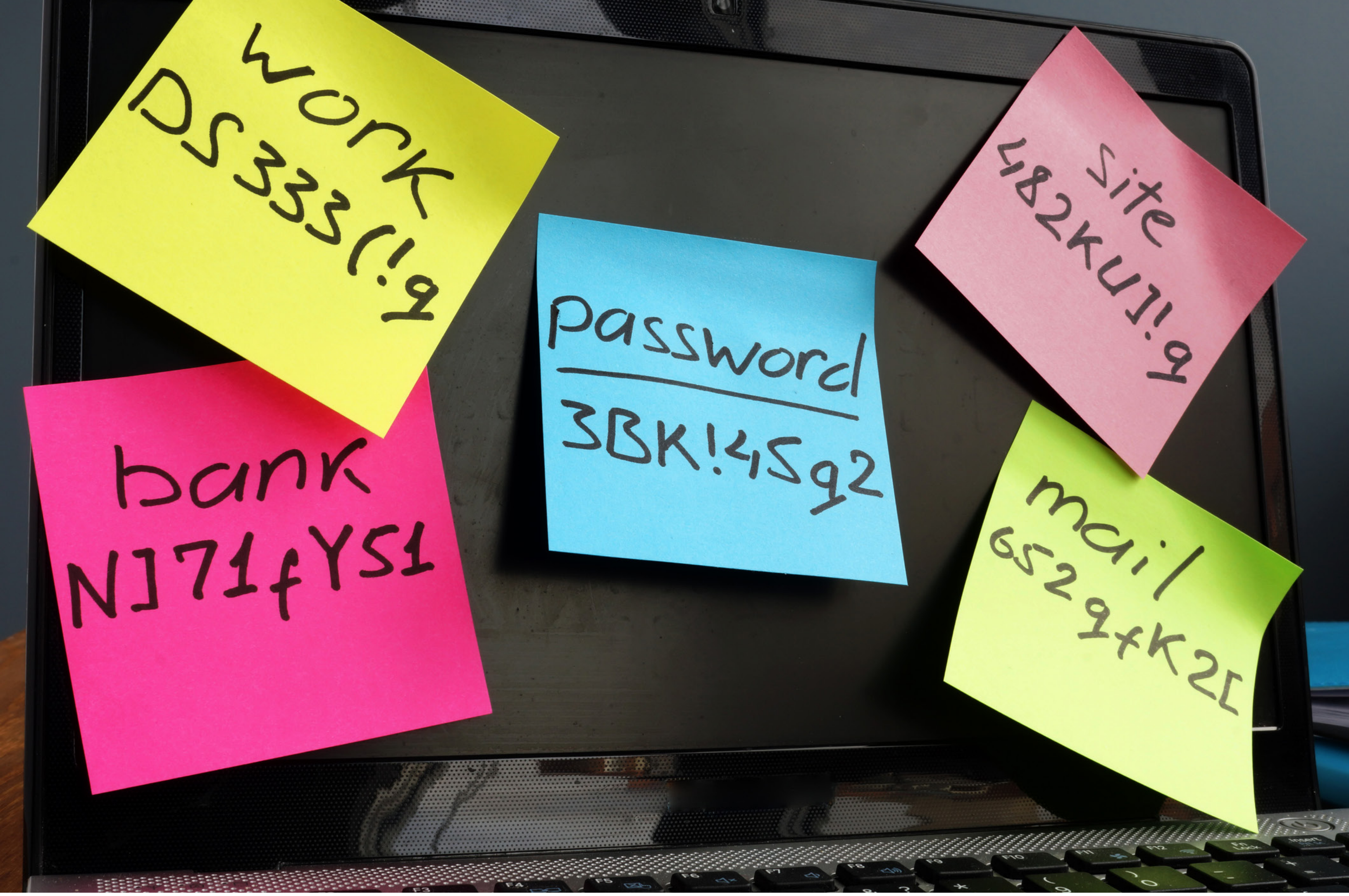


How to manage passwords: Best practices and security tips

TABLE OF CONTENTS

Introduction

Too short, too complex, too frequently used, too many to remember: There are any number of problems with passwords. Individuals can use password managers to strike a balance between security and convenience. However, these services have their own security risks.

This ebook takes a look at pros and the cons of password managers, password alternatives, how to pick a secure password, and more.

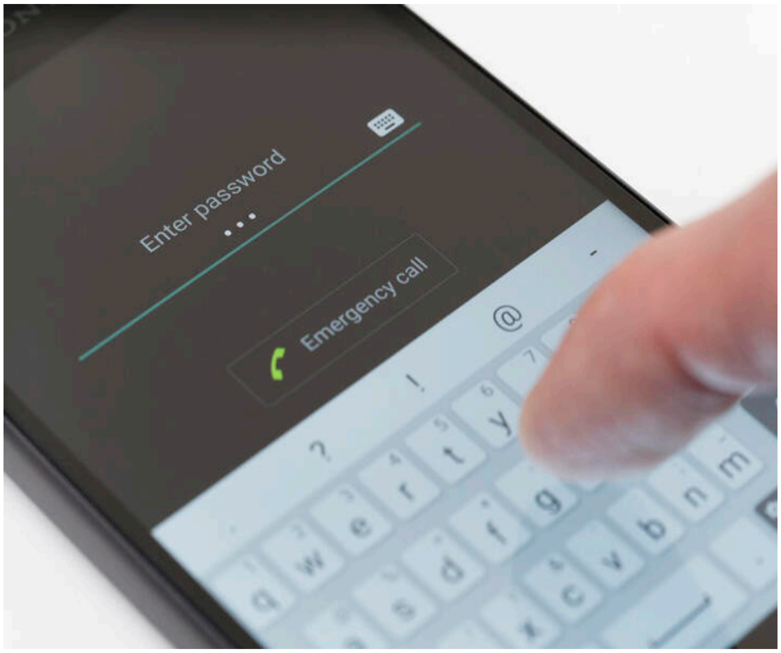
EXTRA SECURITY OR EXTRA RISK? PROS AND CONS OF PASSWORD MANAGERS

Tech consultants and journalists have their own conflicting opinions about the best way to manage access in a world full of security risks.

BY VERONICA COMBS

Too short, too complex, too frequently used, too many to remember: There are any number of problems with passwords. Stanford University now uses digital keys instead of log-in/passwords for students, staff, and professors to access university networks. IT teams are considering password-less solutions to reduce the burden of managing access and identity.

Individuals can use password managers to strike a balance between security and convenience. However, these services have their own security risks. Here are a look at the pros and the cons of password managers based on the experience and analysis of four tech journalists.



ADVANTAGES OF PASSWORD MANAGERS

Rob Pegoraro, a tech journalist, tried LastPass first and then switched to 1Password which offers a free service for journalists. He also uses iCloud Keychain for some accounts and , for some low-value logins, the one Google builds into Chrome and Android. He sees an end-to-end encrypted service as the perfect alternative to remembering dozens of complex passwords.

“A password manager will be a more reliable and secure store than your own head or your browser’s autofill--once you set and memorize a complex password for it and enable its two-step verification,” he said. “That last line of defense can’t be via text message, a channel vulnerable to SIM-swapping accounts; every password manager worth its salt should offer this via USB security keys, which can’t get faked by phishing attacks.”

Pegoraro did add a significant caveat to this endorsement of password managers: He doesn’t keep the passwords for his most important accounts in a password manager.

David Strom, president of an IT consulting firm, has been using LastPass for several years to store hundreds of logins.

“I switch among using a Mac, a Windows laptop, and my iPhone—and I have access to my password collection from all three devices.

Strom said the benefits of the service outweigh the associated security risks.

“As I have a strong master vault password, protected by MFA, I am reasonably confident that I am secure, certainly more secure than reusing passwords across sites,” he said.

Password managers also can help with volunteer tech support.

“As a primary source of tech support for my relatives, I’ve also realized that the secure-notes feature in a password manager is a great place to store the most important passwords of family members in case they forget them or need help with their accounts,” Pegoraro said.

Pegoraro wants Apple to add biometric authentication to a desktop Mac so he doesn’t have to type out the master password every time to unlock 1Password.

“It’s stupid that this Mac-first service is more pleasant to use on my Windows laptop,” he said.

ADVANTAGES OF PASSWORD MANAGERS

After trying several password managers and writing about breaches, tech journalist Sean Michael Kerner takes a low-tech approach to managing his passwords: Paper.

“I have absolutely zero confidence in any password manager, and inevitably there is a risk,” he said. “Paper is low-tech, but it works.”

Kerner uses a YubiKey for multi-factor authentication.

Tom Henderson, founder of ExtremeLabs Inc., does not use a password manager because he sees the companies as prime targets for hacks.

“Relying on them becomes habitual, and they offer a security blanket that’s dangerous,” Henderson said.

Henderson uses four YubiKeys to augment passwords, adding that he knows the owner and founder of the company.

“The convenience factor can be excellent, but having the same key for all possible or reasonable devices can be inconvenient,” he said.

TIPS FOR MANAGING PASSWORDS

In addition to using multi-factor authentication, Henderson suggests keeping passwords and security certificates in a text file with an easy-to-remember name, such as good_recipes.txt or school_dates.txt. Users should update passwords frequently and delete old versions of that file.

“Take a copy on a flash drive and take it off premises so that when the worst happens, you’ll at least have your passwords with you,” he said.

Several writers suggested keeping an eye on HaveiBeenPwned once a month to see if an active password has been exposed.

Strom said that he’d like LastPass to integrate with the site to prevent users from using compromised passwords, a feature offered by 1Password.

5 REASONS WHY YOU SHOULD USE A PASSWORD MANAGER

Need a reason to use a password manager? How about five?

BY JACK WALLEN

IMAGE: ISTOCKPHOTO

This should go without saying. Unfortunately, it does need to be repeated over and over.

You need to use a password manager. Why? Let me cut to the chase and give you five good reasons.

1. YOUR PASSWORDS ARE TOO SIMPLE

This is the biggest reason, bar none. If you're using passwords that you can easily remember (such as password, password123, happyhappyjoyjoy, etc.) you're at risk. Why? Simple passwords are easier to crack. With the right tools (and enough horsepower) a hacker can crack those simple passwords in seconds or minutes. Because of this, you want to make sure that the passwords you use are hard (if not impossible) to remember. A good rule of thumb is that if you can easily remember a password, it's probably easy to crack. The harder that password is to remember, the harder it is to crack. So when you use such difficult passwords, you need a vault to house them. That's where the password manager comes into play.

2. PASSWORD MANAGERS INCLUDE RANDOM PASSWORD GENERATORS

Speaking of complicated passwords, you shouldn't try to come up with complicated passwords on your own, or you'll wind up with variations on your usual theme. Instead, you need a password manager that includes a random password generator to create very complicated passwords. Some password managers, such as Enpass, allow you to configure how complicated the password is. With these tools you can generate passwords that are 20 random characters long or even unpronounceable, random phrases. Make use of these tools, and your passwords will be very complicated and, therefore, strong.

3. YOU ONLY NEED TO REMEMBER ONE PASSWORD

With a password manager, you only need to remember one password--the one used to gain access to your stored passwords. With this in place, you don't have to worry about remembering all those new and highly complex passwords generated by the manager. Open the managing tool, type your vault password, and locate the password you need. The one caveat to this is to make sure your vault password isn't simple. It doesn't need to be overly complex, just not obvious.

4. THE NUMBERS ARE AGAINST YOU

How many accounts do you have which require a password? Tens? Hundreds? The more accounts you have, the more likely the numbers are against you. Because of this, you probably use the same password for everything, which is a HUGE no no. You must use different passwords for every account. With that many different passwords, how are you going to remember them? You're not (especially if those passwords are complicated). That's another big reason to use a password manager.

5. PASSWORDS WILL ALWAYS BE AT THE READY WITH DEVICE SYNCING

Some password managers allow you to sync your password database across all of your devices. With this feature, you can access to your passwords on your desktop, your laptop, and your mobile devices. This way you always have your passwords at the ready. If you opt to use this feature, make sure you have your password database encrypted with a strong password. The last thing you need is for a bad actor to intercept your database and crack it via brute force.

BONUS REASON: IT'S THE WISE THING TO DO

Yes, using a password manager does add a step or two to the log-in process. But when your data and security is at risk, those extra steps are worth it. With each passing day you continue counting on those simple passwords, you run the risk of data theft. Be wise and use a password manager ... before it's too late. RoboForm

5 BEST PASSWORD MANAGERS FOR ANDROID

If you're looking for a password manager for your Android, below are five of the best.

BY JACK WALLEN

In today's world of insecurity, we need to do everything possible to keep our accounts secure. For the end user, that security begins and ends with the password (with a little 2FA caught in the middle). Without a strong password, it's not a matter of if, but when, your account will be hacked. To put hacking off as long as possible, very strong passwords are encouraged.

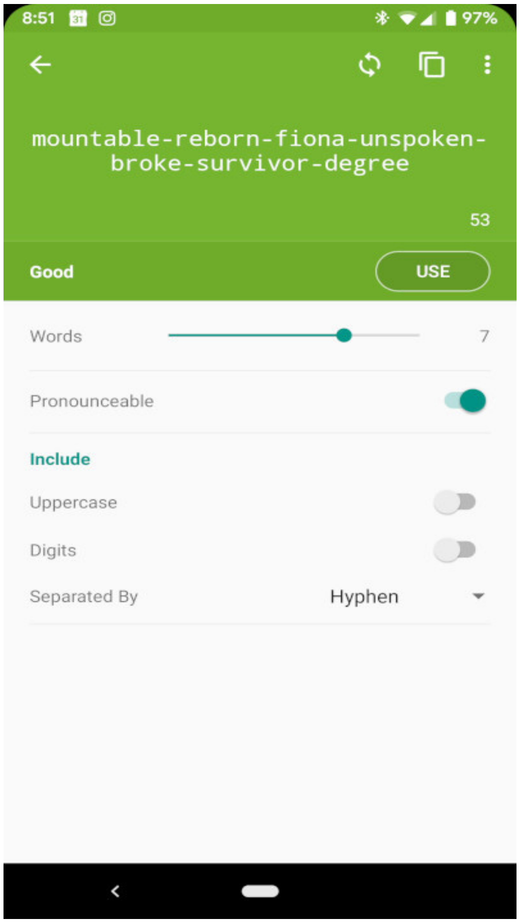
But how do you remember such long and complicated passwords? You don't. You entrust those random strings of characters to a password manager. For the Android platform, there are plenty of tools that serve this purpose. I've cobbled together my list of the five best in this category to share with you. Each was tested on Android Pie or Android Q, but are available for most recent releases of Android.

ENPASS

Enpass is my password manager of choice? Why? Because it does a great job of syncing between all of my devices (it's available for Android as well as Linux, iOS, macOS, Windows, and web) and offers all the features I need to keep my strong passwords safe.

Enpass can create new login entries, has one of the best random password generators on the market (**Figure A**), includes password audit tools, can be unlocked via fingerprint, allows you to tag entries as favorites, includes a tagging system and categories, and much more. The import/export feature allows you to easily integrate Enpass with Dropbox and other cloud services, so you always have a backup of your data file (that also is encrypted). Enpass can be used for free, but the free version is limited to the number of entries. For unlimited access, Enpass is $11.99 USD (one-time fee).

Figure A



mountable-reborn-fiona-unspoken-broke-survivor-degree

53

Good

Words 7

Pronounceable

Include

Uppercase

Digits

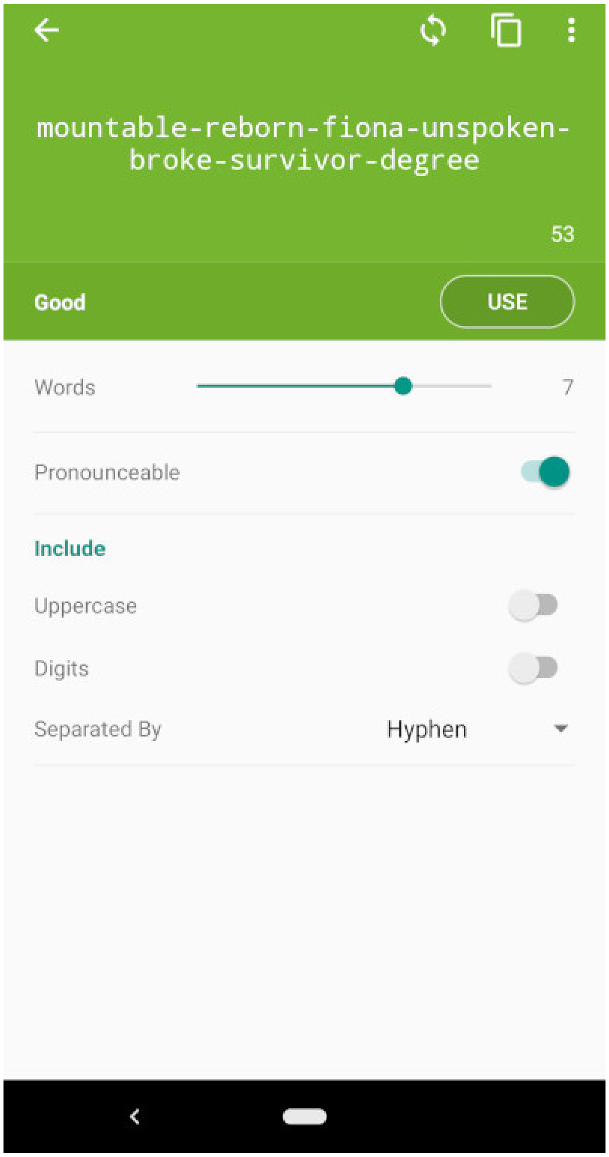
Separated By Hyphen

The Enpass random password generator.

LASTPASS

The LastPass password manager is another fine tool for the job. Although LastPass doesn't include a user-friendly import/export tool (as does Enpass), if you're looking for your first-ever password manager (one that you'll use to start creating new logins), this might be the tool for you. One of the many reasons LastPass finds its way onto this list is because it also includes outstanding browser plugins, that make tasks like autofill and quick login entries a no-brainer. LastPass also includes a Form Fill profile tool (**Figure B**), which allows you to save information (name, address, language, title, username, etc) for when a website works with autofill. You can create multiple autofill profiles, so you can pick and choose which one to use at any given time.

Figure B



mountable-reborn-fiona-unspoken-broke-survivor-degree

53

Good

Words 7

Pronounceable ●

Include

Uppercase ○

Digits ○

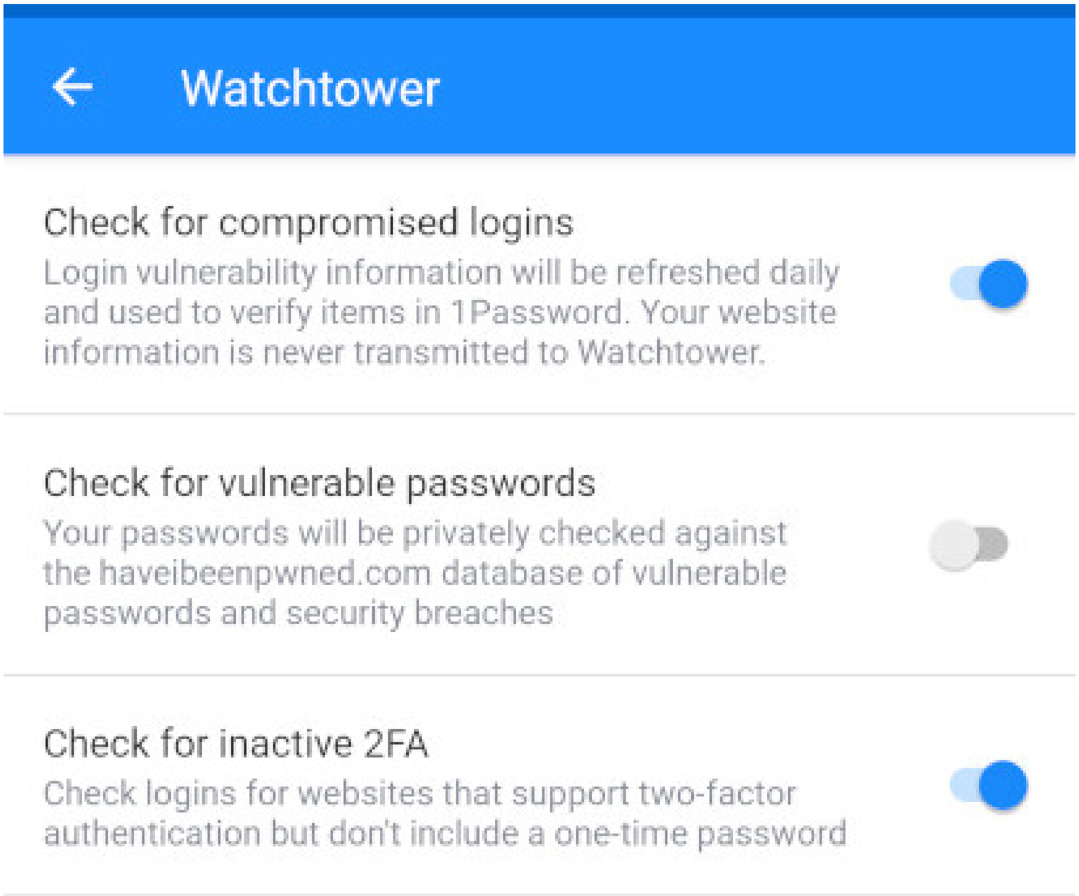
Separated By Hyphen

Creating a LastPass profile for autofill.

1PASSWORD

1Password is another paid password manager on Android, which earns its fee. You pay either $3.99 monthly or $35.99 annually to enjoy this user-friendly, well-designed tool. You can also kick the tires with a 30-day free trial. Once you create your account, you will be given what 1Password calls an Emergency Kit. This is a long string of characters used to sign in from new devices. Without this "kit" you cannot sign into your account from any device, other than your mobile. Make sure to copy and save that string and keep it in a safe place. 1Password includes a fairly standard feature set: Fingerprint unlock, autofill, accessibility, categories, tags, favorites, security audit tools (called Watchtower - **Figure C**), multiple account support, and much more. Although the interface is very well designed, it does take a quick minute to get the lay of the land. New login entries are created from within the Categories tab, so make sure to familiarize yourself with the user interface, before diving into creating entries.

Figure C



Watchtower

Check for compromised logins
Login vulnerability information will be refreshed daily and used to verify items in 1Password. Your website information is never transmitted to Watchtower. — on

Check for vulnerable passwords
Your passwords will be privately checked against the haveibeenpwned.com database of vulnerable passwords and security breaches — off

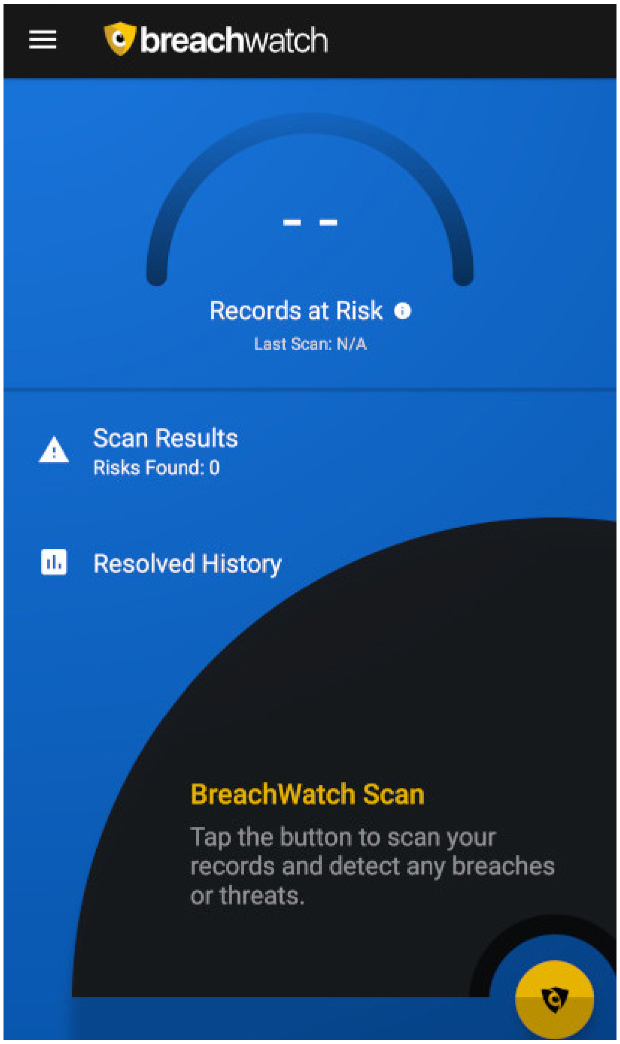
Check for inactive 2FA
Check logins for websites that support two-factor authentication but don't include a one-time password — on

The WatchTower features keep your logins secure.

KEEPER PASSWORD MANAGER

Keeper Password Manager includes a feature that many consumers will appreciate, called BreachWatch, which monitors for stolen usernames and passwords. With a quick tap of the BreachWatch button (**Figure D**), Keeper compares your stored logins with known databases of stolen passwords and usernames. Keeper also allows you to add attachments to entries (such as photos, videos, or other files). You can also add custom fields to entries (which are already fairly inclusive). In addition, Keeper includes a very solid password generator, which allows you to adjust the number of letters, numbers, and special characters, to create as strong a password as needed. Like the above entries in this list, Keeper isn't free. To make use of this password manager, you'll be paying $29.99 per year.

Figure D



The Keeper BreachWatch function at the ready.

DASHLANE

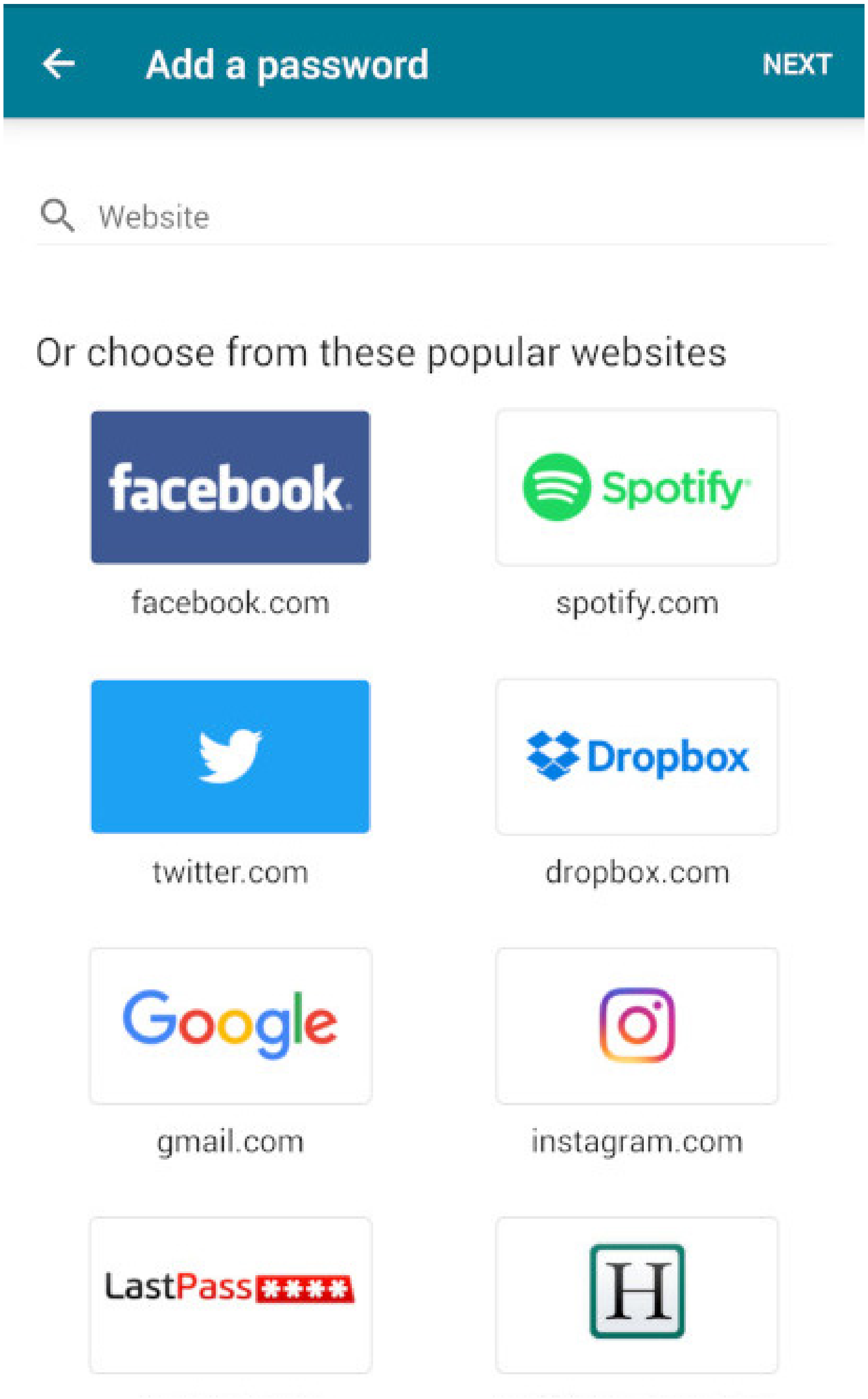
It's time we included a free entry. Dashlane might not have all the features found on the paid apps, but it does have enough to satisfy most users. With Dashlane you can store passwords, IDs, and payment information. Although the app is free, you do still have to create an account (also free).

Dashlane does include a unique feature (that I'm not sure I'd recommend) that stores your most-used password. To those who rely on very strong security, this could be considered a weakness, and should probably be avoided. Dashlane makes it incredibly easy to add password entries for popular sites (**Figure E**). One other caveat is that you must manually set up a PIN code or Fingerprint access to secure the app. Out of the box, you are not prompted for either of these (upon the first run), so make certain you set this feature up (otherwise anyone who has access to your phone will have access to your login information).

MAKE YOUR CHOICE

And there you have it, my entries for best Android password manager on the market. Any of these options will do a fine job of helping you create and protect strong passwords for your login accounts. It's time you made the choice to be better protected.

Figure E



Creating a new login for a popular site is made simple with Dashlane.

TOP 5 WAYS TO PICK A SECURE PASSWORD

Picking a secure password is crucial to protecting sensitive information.

BY TOM MERRITT

Oh, passwords. Someday the FIDO alliance or somebody will save us from them. Until that heady day, we still need them and we need to choose ones that are really hard to guess. Even if you have two-factor authentication turned on--which you should--secure passwords are still a good idea. Fire up your Horse Battery Staple, here are five things to know to pick a good password.

1. NEVER REUSE ONE.

Ever. Data breaches are very common. When your password is breached at a service, that service will usually make you change it. But the service where you re-used it doesn't know that, so you just made that password very insecure.

2. CHOOSE A LONG AND STRONG PASSPHRASE.

Yes, it is possible to remember your password and make it secure. Don't choose dictionary words. Security researcher Bruce Schneier suggests taking a sentence like: "When I was seven, my sister threw my stuffed rabbit in the toilet." And using the first letters numbers and punctuation to make "WIw7,mstmsritt."

3. LET A PASSWORD MANAGER DO IT FOR YOU.

Yes, password managers are a single-point of failure, so be honest with yourself. Are your passwords more secure if you let a manager that is 2FA-protected pick really good ones for you? Or do you want to manage all that yourself? And is the way you manage it, more secure than a password manager? Be honest--nobody else needs to know.

4. DON'T UPDATE IT REGULARLY UNLESS YOU'RE FORCED TO.

It used to be that it took 90 days to crack a password, so if you changed it every 90 days, you could stay ahead. Now it takes seconds, unless you've picked a strong one.

5. SKIP THE SECRET QUESTION.

If that's not an option, answer it like you're making a second password. There's no point in having a really secure password only to have it backed up by a dictionary word in your secret question that's easily guessable.

The fact of the matter is that you should really turn on two-factor authentication and hope that better methods will make the password obsolete. But, until then, I hope these tips help, friend.

TOP 5 PASSWORD ALTERNATIVES

Passwords remain the most common way to authenticate your online identity, but companies like Microsoft and Google are using alternate login methods.

BY TOM MERRITT

Passwords are not yet past, but that glorious future land where we don't have to remember h0rs3##pl7 is getting closer. Microsoft is allowing logins without passwords. Google is allowing logins without passwords. These are secure logins--sometimes more secure than just a user ID and password. Just as a sample, here are five alternatives to passwords.

1. MULTIFACTOR AUTHENTICATION

The right combination of factors means a password doesn't need to be one of them. Facial recognition and a code from a USB key or authenticator app (or SMS, I suppose) could do well without a password. Microsoft uses a PIN as a fallback because it can be stored locally on a trusted platform module.

2. BIOMETRICS

Fingerprint readers for phones are widespread, and facial recognition is getting more reliable all the time. Future biometrics may start to use DNA.

3. BEHAVIORAL RECOGNITION

This one works by taking in multiple data points like typing patterns, mouse movements, software usage, and Wi-Fi networks, and creates a score to decide whether to trust the user for access or not.

4. NOTIFICATIONS

Logging in requires just the username and then a push notification on a phone or an email with a link used as second factor to log you in.

5. CARD AND PIN

From credit cards to grid authentication cards to Estonia's ID, it's the old classic combo of something you have and something you know--neither of them are stored in the cloud to be hacked.

As you can see, multiple factors is the running theme in all password alternatives, and if one of those factors is not remembering a 20-character string of letters, numbers, and special characters, I think we'll all be happier.

CREDITS

Editor In Chief
Bill Detwiler

Editor In Chief, UK
Steve Ranger

Associate Managing Editors
Teena Maddox
Mary Weilage

Editor, Australia
Chris Duckett

Senior Writer
Veronica Combs

Senior Writer, UK
Owen Hughes

Editor
Melanie Wolkoff Wachsman

Staff Writer
R. Dallon Adams

Multimedia Producer
Derek Poore

Staff Reporter
Karen Roby

TechRepublic®

ABOUT TECHREPUBLIC

TechRepublic is a digital publication and online community that empowers the people of business and technology. It provides analysis, tips, best practices, and case studies aimed at helping leaders make better decisions about technology.

DISCLAIMER

The information contained herein has been obtained from sources believed to be reliable. TechRepublic.com, LLC. disclaims all warranties as to the accuracy, completeness, or adequacy of such information. TechRepublic.com, LLC. shall have no liability for errors, omissions, or inadequacies in the information contained herein or for the interpretations thereof. The reader assumes sole responsibility for the selection of these materials to achieve its intended results. The opinions expressed herein are subject to change without notice.

Cover Image: iStockphoto/ designer491