Before You Use a Password Manager

Stuart Schechter Follow
Jun 6 · 26 min read

I cringe when I hear self-proclaimed experts implore *everyone* to "use a password manager for all your passwords" and "turn on two-factor authentication for every site that offers it." As most of us who perform user research in security quickly learn, advice that may protect one individual may harm another. Each person uses technology differently, has a unique set of skills, and faces different risks.

In case you haven't received this advice, or didn't understand what it was, **Password managers are programs that remember passwords for you**, along with the email address or other user identifier you use for each account**. They make it easier to use *strong* passwords**: those that are sufficiently random, long, and different for every one of your accounts. They also **make it easier to lose all your passwords at once**, or for attackers to steal all your passwords in one instant.

In this article, I'll start by examining the benefits and risks of using a password manager. It's hard to overstate the importance of protecting the data in your password manager, and having a recovery strategy for that data, so I'll cover that next. I'll then present a low-risk approach to experimenting with using a password manager, which will help you understand the tough choices you'll need to make before using it for your most-important passwords. I'll close with a handy list of the most important decisions you'll need to make when using a password manager.

There are a lot of password managers to choose from. There's a password manager built into every major web browser today, and many stand-alone password managers that work across browsers. In addition to remembering your passwords, most password managers will type your password into login forms. The better ones will create randomly-generated passwords for you, ensuring that you're not using easily-guessed passwords or re-using passwords between sites. Some will even identify passwords you've re-used between sites and help you replace them.

Password managers help protect your passwords

Password managers protect you by creating a strong, unique password for every service you use, and removing your need to enter those passwords.

Password managers can prevent password-reuse attacks, in which attackers break into a website, steal users' email addresses and passwords from it, and try to login to other sites using the email/password pairs they stole. The attacks work because many people re-use the same password on multiple websites. Password managers makes it possible and easy to use a different random password for every account — at least once you've replaced all your old re-used passwords. The replacement step is important because if you leave all your old passwords in place, and just let the password manager enter them for you, the password manager can' stop this attack.

Password managers can prevent impostor websites from "phishing" you. Impostor websites are designed to look like a website on which you have an account, in order to trick you into entering your password for that account. Attackers often craft emails to appear as if they're coming from the website they want to impersonate, but provide a link to the attacker's website. Password managers protect you from these attacks because they will not enter your password if you're at the attacker's website. If your password manager knows your unique random password for that site, but you don't, it's much harder to be tricked into entering it [1].

Password managers track which services you have accounts with, helping you identify unused accounts that you may want to close or delete data from to reduce your online exposure.

Password managers can also put passwords at risk

The old proverb about keeping all your eggs in one basket applies to password managers; yes, you can focus on guarding that one basket, but it just takes one mistake to lose all your eggs [2]. (If this thought of risking all your passwords at once makes you want to stop reading and give up on password managers now, don't! In the section that follows, I'll explain how password managers can be helpful even if you don't entrust them with all your passwords.)

How might you lose all the passwords in your password manager at once?

You may forget the master password that protects your other passwords. Once you've

replaced your passwords with random passwords, and relied on your password manager to enter them for you, you're unlikely to be able to remember many of them anymore — the initial selling point of password managers was that you shouldn't have to. If you lose the master password that the password manager uses to protect your other passwords, you could lose everything. There are recovery options, but none is perfect, as I'll discuss later.

An attack on your password manager can reveal all your passwords. This includes attacks on any device on which you store you managed passwords. Even if you've locked the password manager, an attacker will be able to get to them when you next unlock it on that device. Many of the password managers that offer a "locked" mode, in which you can turn off your device's access to your passwords, but most are vulnerable to an attack that can unlock your passwords the moment that malware gets on your machine [3].

If your personal laptop is infected with malware and you use your password manager on it, the malware can read every password you keep there. If you use your password manager on a work computer, anyone who has administrative access to that computer may be able to compromise your passwords in your password manager — even for sites you never log into from work. If you use your password manager on a tablet and leave the password manager unlocked, anyone with the tablet can access all your passwords. If your phone is stolen, if the thief is able to unlock your phone, and if you don't have your password manager configured to require unlocking with every use, the thief now has access to all your passwords.

In contrast, if you don't use a password manager and your device is infected with malware, and attacker can steal the passwords you type, but not the ones you don't. You can decide that some passwords are okay to type on lower-security devices, but others should only be typed on higher-security devices.

Lastly, a password manager is yet another piece of software installed on your devices that could become compromised. All software has bugs and, despite being developed to meet a security need, **password managers have been far from immune to security bugs**. It's hard to know which is best because I have yet to read product reviews for password managers with meaningful ratings for security [4].

. . .

You can start without risking high-value passwords

If the above risks make you reluctant to use a password manager for *all* your accounts, consider starting with those passwords that you would least worry about losing or being compromised.

For example, you probably don't care about a password used to create a seven-day trial subscription to a software program, news articles, or research. If you shop at many different websites, you might have dozens accounts which all protect copies of the same information: your credit card number, phone number, and address. None of this information is very secret, your liability is limited if your credit card number is stolen, and it's easy to reset the password for most shopping sites by receiving a password-reset email.

By starting with your lower-value passwords, you can familiarize yourself with how password managers work while the consequences of mistakes are low. As you gain experience, you'll also better understand the risks and benefits. You may find that when you no longer have to create, remember, and type those lower-value passwords you can put some of that saved effort into protecting passwords for higher-value accounts.

You can also use your password manager to generate random passwords that you shouldn't save. You'll probably want to write those down. You should be able to learn random passwords for a few accounts over time just by using them.

Most users can get started without buying or downloading new software. If you primarily use Safari or Chrome, both browsers have password managers that will generate random passwords for you. I'm not going to cover Brave, Edge, or Firefox because, at the time of this writing, they don't generate passwords.

While you should consider stand-alone password managers, especially if storing passwords for your more valuable accounts, you can easily import into them the passwords you saved while trying out the built-in password managers in Chrome or Safari.

One reason to move beyond Chrome is that it will not identify which passwords you have re-used between sites [5]. Auditing for re-used passwords is essential to getting the security benefits a password manager can offer. Most stand-alone password managers offer an audit feature, and Safari's built-in password manager (Apple's Keychain) recently added one as well.

Even if you try not to store important passwords in your password manager, it's still worth periodically reviewing which passwords you've saved and which are re-used — some accounts that seemed valueless when you created them may turn out to be more valuable over time. Some password managers will also point out if some of your passwords are obviously weak (e.g., if they appear on common-password lists.) If you want to replace your old passwords, the amount of work may be daunting. You don't have to wait until you have enough time to change them all at once; prioritize and get started.

Alas, password managers that test whether you've re-used a password will only do so if you allow them to store that password. If you only store passwords for low-value accounts, the password manager will only be able to tell you which of your low-value passwords have been re-used. I know of no password manager that will alert you if you type a password you've saved for another site into the current webpage [6] [7]. There's no technical reason most password managers couldn't alert you to such password re-use, so I hope some will soon.

Learn a strong master password

Most password managers protect your passwords with yet another password —commonly called a *master* password. Stand-alone password managers will ask you to create a master password when you start using them. If you use Google's Chrome browser to store your passwords and share them across devices, your passwords will be stored by Google and protected by the password for your Google Account (along with any second factors you may be using). Apple's iCloud Keychain relies primarily on your device passwords and unlocking features to protect its data on a regular basis, but has a fallback master password called an iCloud Security Code [8].

Don't use a master password you have used for anything else. This bears repeating because you've probably learned to warnings against password re-use having received such advice for accounts you don't care about. Unlike those valueless passwords, the master password that protects all your other passwords really should be unique.

If you're using the Chrome password manager sync'd via your Google Account, and are not 100% certain that your Google Account has a strong and unique password, create a new one (after making sure you have a recovery plan for if you forget that new passwords, as discussed below). This is also a good time to re-evaluate whether you should have two-factor authentication for that account. Similarly, if you're using Apple's iCloud Keychain, don't reuse a password as your iCloud Security Code.

Your master password should be randomly generated and long enough to protect your password even if attackers get hold of a website's encrypted password list and try to break that encryption. To ensure your password is truly random, let your password manager generate it (or use dice and a word list). Many people falsely believe they can generate randomness by summoning letters to their mind or pounding on their keyboard, but many of the mental processes we think of as random actually aren't truly random. A good password manager will use a cryptographic random number generator to ensure your password is sufficiently random (and dice are a time-tested source of physical randomness that you can check for fairness simply by rolling them).

Your master password should be at least 12 lowercase characters or five words. Why use lowercase characters or words when you've probably been told (and coerced) to use uppercase characters and symbols in the past? If you have to enter the password on a device with on on-screen keyboard (like your phone's), each uppercase letter or symbol may require extra key presses. You can get the same security, and save yourself a great deal of frustration, by making your all-lowercase password just 30% longer than if it were mixed case [9]. In other words, a randomly-generated 13-character lowercase password, which can be entered with 13 keystrokes, is as secure as a 10-character mixed password, which may require many more.

Don't expect to learn your new master password immediately — very few people can learn a long randomly-generated string in one sitting. Rather, the best way to learn your master password is to write it down and use it often. Configure your password manager to require you to re-enter it at least once a day until you know it, and only dispose of your paper copy after you've reliably entered it from memory for many days. While people's ability to learn random passwords isn't well studied, research my collaborators and I have performed suggests that it will take between 10 and 30 uses to remember it. (That research investigates techniques password managers could use to help you learn strong master passwords, but none currently offer any help.)

Finally, don't assume you won't lose your paper copy of the master password before you've

memorized it, or that you won't forget later.

Factor recovery into choosing a password manager

Since the one of the biggest differences between password managers is process to recovery your data if you lose your master password, you shouldn't choose a password manager without researching its emergency recovery process. After you make your choice, the first thing you should do, along with choosing your master password, is to set up this recovery process. You may need it very soon, as you are most likely to forget a master password shortly after creating it, and before you have learned it through repeated use.

While the consequences of losing your passwords may seem small when you're setting things up, and don't have any saved passwords to lose yet, you may quickly become dependent on your password manager. You might incorrectly assume that, once you've learned you password, you'll never forget it. While it's most common to forget passwords shortly after creating them, it's also common to forget them after a period of not using them. For example, you might forget after that next vacation you have planned, or, as a friend learned a few years back, after an unplanned hospital stay.

Why does every product handle recovery differently? In part, because it's a really hard problem even for companies that are among the world's biggest, best funded, and best known for great usability. Consider Apple's iCloud, which stores the iCloud Keychain used by Safari. One way to recover an iCloud account is via customer support, but hackers have tricked support agents into compromising user accounts, including for a high-profile reporter in 2012. So Apple also offered users the option to store a randomly-generated password to use for recovery (Apple called this a Recovery Key) and configure their accounts so that customer support could not change their password. Few users adopted recovery keys, and some who did were upset when they discovered that, in fact, customer support could no longer help them when they needed it. Apple stopped offering Recovery Keys in 2015 [10]. Apple currently allows passwords to be reset after verifying customers via their phone number, despite this process being quite vulnerable to attack.

If that weren't bad enough, the requirements that determine whether customer support will reset a user's password or other credentials are not available to the public. Of companies that allow customer support to reset users' account credentials, I know of none that share the rules they use to make decisions about what is required to get back in. Without those rules, users can't know the conditions under which they will be able to recover their account and under which conditions an attacker can take over their account. It's worth repeating this: these companies expect you to trust them with your account but won't tell you the rules that dictate whether you will continue to be able to access it or whether an attacker can steal it from you [11].

Rather than rely on opaque customer support rules, many password managers use solutions that are less vulnerable to attack, but more vulnerable to accidental loss.

Open source password managers KeePass and PasswordSafe (the original password manager) leave it to you to find a way to store and backup the file containing your passwords, along with the key used to protect (encrypt) the data in those files. So, if you want to share your passwords between machines, you'll need to create an online file storage account (e.g. DropBox). Your backup could be a written copy of the master password and the password for the file sharing account. If you use two-factor authentication on that account, you'll need a backup for that too.

LastPass, Keeper [12], and Dashlane let you pre-authorize emergency contacts to access your account…so long as they also have an account with the same password manager. That requirement is in place because these products use cryptography to ensure your friends, but not the companies, will be able get get access to this data. This helps protects you if their service is hacked or if an attacker successfully impersonates you to their customer support staff. The downside is that an attacker who compromises your contact's account may then be able to compromise yours. You can reduce the chance of that happening by putting a time delay before your information can be released to your emergency contact. If you know people using one of these products who you would trust to be your emergency contact, that product may be better for you than the ones which your contacts don't use.

With 1Password, your master secret is actually in two pieces: a secret key, which the software stores on every device you've put your passwords on, and your master password. To use a new device with 1Password, you have to transfer your secret key to it. You can backup your secret key by generating an "emergency kit", a PDF which you can print that contains your secret and space to write down your master password. (Hopefully your handwriting is better than mine.)

Like LastPass and Dashlane, 1Password has designed their online service so that they don't keep these secrets and so customer support cannot help an attacker — or you — get access your data without them. Unlike LastPass and Dashlane, their recovery process doesn't require any interaction with the service, or anyone else. This makes 1Password arguably the most private option, but there's a cost to every customer having this level of privacy: 1Password can't know what fraction of customers have printed out recovery kits, how many have successfully used them, nor how many have lost their passwords forever. The only data they get to help them improve the reliability of their recovery process comes from what users volunteer if they contact support.

If you're using Chrome with a Google Account and two-factor authentication, you can get ten one-time-use recovery passwords (eight-digit numbers they call backup codes) which can substitute for one of your two factors [13]. Google recommends that you "print or download" these. Google also stores these codes and so, unlike well-managed randomly-generated passwords, your codes could be compromised if Google suffers a breach.

If you use a printed recovery secret with Chrome or 1Password, or if you create your own for KeePass or PasswordSafe, you'll need to decide where to store your recovery secrets after you print them. A safe deposit box or a home safe may be appropriate, especially if you already have one or need one anyway. There's no technical reason you couldn't share printouts of your recovery secrets with friends. If you were to, you might not want the sheet to say who it's for, as excluding that fact might provide a small amount of defense if it's stolen. Another option is to give two trusted contacts half of a code, or three trusted contacts two thirds of each code (so that any two contacts could help you).

If you don't like any of the above options, you could print all your passwords periodically or write them down. If you print, you'll be relying on your printer being secure and having a safe network connection to that printer.

Your primary email password also requires special consideration when planning your recovery strategy, since many other passwords can be reset by email. This may be the most important password to change to a randomly-generated password, but it's also the one you'll need the most of you lose access to your password manager. If you're changing that password, you should considering writing it down or backing it up as well.

. . .

Think carefully before storing high-value passwords

Once you want to start storing passwords that have value, the decisions get harder and the answer that's right for one person may not be right for another.

The first decision will be which devices get access to your passwords. Given how often you probably use your phone, and how painful it is to type passwords on a phone, you'll probably want to sync your passwords to your phone. If you do, all your passwords will now be stored on your phone. You may want to review how quickly your phone will lock after you stop using it, and what mechanisms you will allow to unlock it. If your kids or partner know your PIN, do you trust them with all of your passwords as well? If people who you wouldn't trust with all your passwords know your PIN, you could use a stand-alone password manager that has a second unlock mechanism after you unlock your phone. Are you willing to do the extra work every time?

You'll have to make these decisions for not just your phone, but *every* device you type passwords on. For that shared family tablet, you'll have to decide between installing your password manager or having to tap in the new random password you created for your Netflix account while your daughter screams in tears waiting for the latest episode of Mermaid Engineering Squad.

Do you install your password manager on a work laptop that everyone in IT has access to? If you spend most of your time at the office, you probably end up doing a lot of personal computing on your work devices even if you'd rather be doing them somewhere else.

Do you install your password manager on devices you only use every once in a while, and thus may not be getting security updates as often as you'd like? What about laptops you install lots of random software on? What about a laptop that your family members can also install software on? Are you willing to hand copy the valueless passwords you need to use on these devices over from a device you trust with *all* your passwords?

How will your password manager interact with your two-factor authentication strategy? If you

use a two-factor app on your phone, and your password manager is on your phone, are you comfortable with your phone now being both factors? I would be caution against using your password manager to store second-factor codes, as your password manager will become a single point of failure for both your password and these codes. However, if both are on the same device, that device is already a single point of failure.

You'll need to decide whether to save passwords for high-value accounts. As I mentioned earlier, you can use your password manager to generate random passwords for your high-value accounts regardless of whether you choose to let the password manager save it or not. If you have already memorized strong unique passwords for these accounts, the biggest reason to add them to your password manager is to avoid accidentally typing these passwords into impostor websites.

To get that protection, your password must be shared with every device that your password manager is installed on, and unlocked whenever you need any one of your other passwords. In other words, you must decide if you're willing to trade off an increased risk of your password being stolen from your password manager, and the devices you've installed it on, in return for the protection the password manager gives you from "phishing" attacks, as well as the convenience of having it remember and enter the password for you.

The right answer depends on which attack *you* are more likely to be vulnerable to and — let me say this one more time — everyone is different.

If you spend most of your time in a web browser, and primarily use operating systems that sandbox all software (e.g, iOS & Android), falling victim to an impostor website may be relatively more likely and you may want to opt for a password manager. If part of your job is to evaluate which software package may best solve a problem and you spend most of your time in Windows or MacOS, infection by malicious software may be relatively more likely.

The specifics of the account matter too. If it's an account you would use every day, and would have to type every day, then if your computer is compromised an attacker won't have to wait long until seeing you type it again. In that case, saving the password in your password manager might not be adding much risk. If you only use that password on your safest device, and rarely at that, then adding it to a password manager may greatly increase the risk that it will be compromised along with one of your devices.

I'd love to be able to provide great data on the prevalence of these different attacks but, sadly, such data is hard to come by. Some attacks are over-reported, some are under-reported, and some are not discovered at all. There's no shortage of bad data from sources that have an agenda or are selling something. (Take, for example, popular statistics about the fraction of people using "dumb" passwords, which often use statistics from breaches of valueless accounts that aren't worth using good passwords for.)

Even if great data were available, every user is different from other users, and every one of your accounts is different. There is no one-size-fit-all answer.

. . .

Summary

You may be doing more harm than good if you install a password manager, let it store your old passwords, and don't take advantage of the features that can actually improve your security.

Password managers can only protect you from attacks on re-used passwords if you're willing to let them replace your old passwords with randomly-generated unique passwords. They can also best protect you from accidentally entering your passwords into impostor ("phishing") websites if only they, and not you, remember your passwords for the accounts being targeted. So, if you are getting a password manager to improve your security, you'll need to let the password manager replace passwords you've already memorized with random ones.

To reduce the risk of losing all your passwords at once, you'll need a strong master password and a reliable recovery strategy. Choose a password manager with a recovery option that works for you, configure recovery *immediately*, and strongly consider learning a long random master password generated by your password manager. You probably don't want to store your higher-value passwords until you have memorized your new master passwords (this could take weeks) and have your recovery plan in place: if it relies on trusting people, make sure they understand and are comfortable with that role. If recovery relies on your ability to get your hands on an object (e.g. a printed code), choose a place you feel it is safe to store it.

Since there are a daunting number of factors to consider and decisions to make before using a password manager, I'll close with a list that you can use to help ensure your decision is an

informed one. I hope you find it useful!

. . .

Decisions to make when using a password manager
Which password manager will I use?
How will I recover access to my passwords if I lose my devices and/or my master password?
How will I store store my master password until I memorize it?
Which devices should I install the password manager on?
Which of those devices will need a stronger authentication mechanism to ensure someone who uses or steals that device can't get all my passwords?
Which of those devices need stronger security measures to protect against malware that could steal all my passwords?
Which of my passwords should I not risk storing in my password manager?
Which of my accounts should I have my password manager create new, random passwords for? (Don't forget that you can have it generate, but not store, passwords for accounts you don't want it to manage.)

. . .

The password managers discussed in this article along with the features that most impact security and your ability to recover access should something go wrong. See the footnotes for additional information [14].

. . .

If you found this article useful, you may also appreciate its predecessor, "Before you turn on two-factor authentication".

About the author *Hi. I'm* ***Stuart Schechter.*** *I spent over a decade of scientific research rigorously testing the human factors of security technologies while at Microsoft Research [15], MIT, and Harvard. I'm currently brewing new authentication technology for backing up password-manager data and second factors [16] from deep within Seoul's plastic surgery district. To learn more about them, please follow me on twitter (@uppajung). More importantly, if you don't follow me on twitter, my daughters will continue to accumulate a larger social media following than mine at less than a third my age.*

I would like to thank Lorrie Cranor for encouraging me to write this article and initial feedback. I would also like to thank Lujo Bauer, Jon Callas, Cormac Herley, Wladimir Palant, Jeffrey Goldberg (of 1Password), Dominic Battre (of Google), Mallory (@stommepoes), and Jesse Kriss for providing feedback and fact checking.

. . .

End Notes

[1] An impostor website may still trick users to retrieve the password from their password manager and enter it by hand.

[2] There are other alternatives between managing all your passwords on your own and guarding them all with a single master secret. For example, you could memorize two strong master passwords to separate passwords you want on all your devices from your most valuable passwords. Alas, none of the password managers I've looked at offer this feature. Dashlane does let business customers separate business passwords from personal passwords, but they're still all unlocked using the same mechanism, so it's not clear what additional security this provides. 1Password allows you to separate passwords into multiple vaults, primarily for sharing passwords with others. However, 1Password does not allow you to use different master passwords for your different vaults, noting that this would be "inconvenient" and off brand. LastPass allow you to divide up passwords into levels via their *Identities* feature under the same master password. You can then use your master password to unlock a limited set of passwords on a device, such as before handing it to someone else. However, it doesn't protect you from malware that is resident on your device when you enter that master password.

[3] In fact, even if your password manager is locked, it may still be possible for attackers to extract the passwords, as detailed in a report by Independent Security Evaluators.

[4] I came across many password manager product reviews in writing this article. Those that provided a security rating gave little justification for their scores, or were simply counting up which had more features they could count as security. Some of these features (e.g., support for two-factor authentication) did not have a clear connection to increasing the security of users' passwords. An actual review of security would note whether the company producing the password manager provides a detailed public description of its security architecture (e.g., this one from 1Password), the choices made in that architecture, the number and severity of security bugs have that been reported by security researchers, and the speed at which security bugs get fixed. They should also review findings from independent auditors such as Independent Security Evaluators.

[5] Google offers a browser extension to check if the username and password pairs you've saved have been compromised. However, it does not provide a feature to identify password re-use before the compromise.

[6] Cormac Herley, a former colleague at Microsoft Research, proposed such a feature over a decade ago, using an approach that would allow you to check if passwords you weren't comfortable saving were re-used.

[7] One way to check if you've re-used an important password is to disconnect your device from the network (to prevent the password manager from saving your password there), adding the password to your password manager, checking if it is among your re-used passwords, and then deleting it before turning networking back on. Yuck!

[8] In Apple's iCloud Keychain, each of your devices shares a master key used to encrypt your passwords before they are uploaded to iCloud. Your passwords are protected on each device by whatever means you use to unlock the device. You can add your Keychain to a new device by having one of your existing devices approve the addition, which transfers the key from that device to the new device. A separate secret, your iCloud Security Code, can recover your Keychain from iCloud if you lose access to all the devices it's stored on.

[9] This math is based on the 26 characters in use in English,10 digits, and about 8 symbols that can reasonably be expected to appear on all the keyboards you might need to enter a password with. Each randomly chosen character from among the 26 lowercase characters used in English provides 4.7 bits of security. Doubling the number of characters used, such as by adding the 26 uppercase letters, adds only 1 bit. Adding in the additional 18 characters (for a total of 70 characters) yields 6.13 bits, or only 30% more.

[10] I've heard product managers from a similarly-sized company complain that only a tiny fraction of users create backup passwords and print them.

[11] The most common justification for not revealing the processes by which customer support

determines whether to reset or not reset account credentials is that attackers would benefit from this information. This justification violates a principle security practitioners adhere to in other contexts, that the security of systems shouldn't rest on the secrecy of their design (Kerckhoffs's principle).

Keeping attackers in the dark isn't the only reason that companies aren't transparent about the rules their customer support teams follow. These rules may change frequently and, for better or worse, companies may want to leave some decisions to their staff's discretion and intuition.

Also, if a request to restore access to an account from a person of influence, such as a politician, social media celebrity, reporter, or even a friend of an employee, companies may use their employee's relationships and networks to verify the authenticity of the requester and help them out. The cost of reaching out through the personal relationships of company employees may be small relative to the value of a key influencer's gratitude. Influencers tend to be easy to reach (*when* they want to be reached) as they are socially well connected and have well-known business associates.

Companies cannot offer the same level of service to everyone. Most people are harder to reach, and companies would grind to a halt if their employees' personal relationships were constantly being tapped to help every customer who needed an account recovered. By keeping how they operate opaque, companies have been able to avoid press scrutiny over preferential treatment of influencers, while at the same time enjoying the gratitude of those members of the press who have benefited from the privilege of their influence.

With this in mind, when someone tells you that you should "use a password manager for all your passwords" and "turn on two-factor authentication for every site that offers it," and assumes that what works for them should work for you, you might want to ask if they have they have friends at the companies who operate the accounts they'd need to regain access in an emergency.

[12] Keeper also offers recovery via a security question, and encrypts your recovery secrets with the answer. I recommend against using it. Collaborators and I researched user-chosen security questions over a decade ago, and our results did not indicate this approach was anywhere near reliable or secure enough for such use — many participants and choose questions with answers that were too easy to guess and many weren't able to recall their answers later.

[13] At least that's how I think that's how it works. Their support pages leave out details and some of the details and, when I tried to verify some of the details on the support page, some turned out to be incorrect. (I reported this to my contacts at Google, who have filed a bug report.)

[14] Notes on the figure:

A site "verifies that [a] site isn't impostor" if the password manager will fill/type a password for you, but only if it is on the correct site.

Your data is "blinded to customer support" if the service is designed so that the company/organization that wrote the software so that it can't see users' passwords or change who has access to them. Companies like Google and Microsoft put extensive measures in place to prevent customer support from seeing your passwords, but since customer support can help "recover" accounts, they could also accidentally help an attacker steal them.

KeyPass does not have a built-in mechanism to auto-fill passwords (key to protecting against impostor websites) or to identify re-used passwords, but offers "extensions" to do both.

There are at least three features I will include if even one password manager offers them: (1) allowing users to partition passwords under different keys, (2) checking if a password currently into the browser is the same as one saved for another site, even if the user chooses not to save the current password, and (3) training that helps users learn their random master password over time.

For more information, there are security architecture descriptions from 1Password, Dashlane, Keeper and LastPass. PasswordSafe is open source and has online documentation of much of its security architecture.

[15] Some readers might complain that, as a former Microsoft employee, I have not scrutinized Microsoft's Edge browser and its built-in password manager, a product of my former employer, with anywhere near the level of scrutiny I've given to Apple's Safari Keychain and Google's Chrome. I have not done that because the password manager in Microsoft's Edge will not generate random passwords, and so is ruled out as not worthy of consideration early in this article.

[16] A note regarding conflicts of interest I was able to write "before you turn on two-factor authentication" at a time when I had no financial interest in any authentication technology.

Since then, and in part due to the reception that work received, I started developing tools to help users backup and recover the secrets they use for authentication. This, and ten years of research on account recovery that is routinely ignored by practitioners, may have colored my opinion about the current state of the art.

Security Passwords Password Manager

WRITTEN BY
Stuart Schechter
Follow

See responses (5)