ENG 253 Module 2 Portfolio

Michael Garcia

November 2022

Contents

1 Cover Letter

Preface

Writing for different audiences, you had to take into considerations the vocabulary and semantics in the fashion that they are used in. Someone once said that if you are not able to explain a subject to a six year old, you may not understand it yourself. I took that literally and the individuals I have worked with to cultivate three different documents all of which have a different target audience in mind.

For the informational text, I tried my best to form the linguistics to conform to less tech savvy individuals who may be trying to explore new ways to stay secure. My idea is, if a individual is curious enough to stumble upon a password manager, the rest of the information should follow along the same pattern of curiosity without sounding too obnoxiously technical. I chose to write in the format of an instructional manual because I find it aesthetically appealing and useful. It's effective as introductory manual because it summarizes how to get started with using the service and answers a few questions for those who are still hesitant.

As for the analytical memo, I had to recreate this to a different organization where I am at the helm of IT. The analytical memo targets an audience of office workers who should know a thing or two about using office tools. Moreover, this is an effective text because stakeholders in an organization will be concerned if this really necessary, and I believe the included statistics should hold the argument sound. In this text I need not to persuade, but to inform.

Finally, the op-ed had to be completely overhauled as it came out to be more of an information text than an op-ed. For this piece I chose to target a educated audience who are more concerned with the techno-political climate. Users who are enthusiastic about technology but are upset that they are not being protected. I aimed to educate readers on some history and why cybersecurity in an organization is difficult. Additionally, I had to ensure the reader that there are some progress being made to reel them into the next part which is for them to take action to further cement the idea that legislation can help cybersecurity in an organization. I think this text is effective in the way it has conveyed so much information in a short span of pages. In the scope of cybersecurity, I managed to cover who is affected, why it happens, who the responsible parties are, what has been done to remediate the situation, and what do we need to do now. I consider this piece of text to be my magnum opus for this course (perhaps a few tweaks are still needed).

2 Informational Text

Getting Started with 1Password Password Manager

Version 1.1

Michael Garcia

November 28, 2022

Contents

1 Introduction

1Password is a password manager that is designed to help you manage all your important digital accounts. Store your logins and other important digital credentials in a user-friendly and accessible platform that you can access on your Windows, macOS, Android, iOS, and ChromeOS device.

To keep your information secure, we have zero-knowledge of your passwords. We collect only the information necessary to provide our services and assist you in troubleshooting. We collect information about:

- **Your 1Password account**: What kind of account you signed up for, who owns that account, and how that account has been paid for.
- **Your usage**: When you log in, how many vaults you create, how many items are stored in your vaults, and how much storage space you use.
- **You**: Your IP address, the devices connected to your account, and the name, email address, and profile pictures that you have given to us.

1.1 Master Password and Secret Key

To access your account, you'll be given two responsibilities: the master password and your secret key. Your master password is something you know, this is the only password you'll have to know, we'll remember the rest. The secret key will be something you have, this is the second password key needed to access your 1Password account. You don't need to remember or carry around your secret key but it is important for you to keep this information somewhere safe and secure. You only need to enter the secret once for a new device you are registering for 1Password.

2 Getting Started

1. Sign up on 1Password.com.

   You'll get an email to confirm your account. Then you can choose a strong account password, which you'll use to unlock 1Password (this is the master password).

2. Download our application on 1Password.com/downloads.

3. Add new or move over existing passwords.

   If you have existing passwords on other password managers you can follow our guide on support.1Password.com/import

3 FAQ

- **How does 1Password work, and why should I be using it?**

  1Password allows you to create a single account password that secures all your other passwords. Then you can use strong, unique passwords for all your online accounts, which means a security breach on one website only affects that one site.

- **How secure is 1Password? Can I trust 1Password?**

  The 1Password Security Design [1] explains exactly how your secrets are kept safe. It's a lot to read, but it covers all the inner working of 1Password if you want to learn more.

- **Would it be safe to store all my credentials under one umbrella?**

  Your 1Password account is kept behind a secure encryption. Your password and secret key together make it computationally infeasible to decrypt your information without the proper keys. Therefore, it is important that you keep your password and secret key secure and known only to you.

- **Can 1Password create passwords for me?**

  Yes, 1Password can create strong passwords that are unique to every account. All your accounts should have a unique password, 1Password makes that easy.

- **Do I have to fill in my logins every time?**

  No, 1Password has an autofill feature that can fill in logins for you inside apps or websites.

- **Can I still login if I forget my password and secret key?**

  If you forget your password or secret key, we would be unable to recover your account. It's important to keep the backup of your secret key somewhere safe and secure. Your master password should also be stowed away somewhere safe.

  If you happen to lose either your password or secret key, you may try recovering your account through another device that still has access to 1Password. If you don't have any access whatsoever, recovery is not possible.

- **If I login in one device, can I access the same information in another?**

  Yes, all your information is synced online and the encrypted information is stored in our servers.

4 Revision History

Revision Date	Version	Name	Changes
10/16/2022	Version 1.0	Michael Garcia	- Initial draft.
11/25/2022	Version 1.1	Michael Garcia	- Re-written in LaTeX formatting. - Mass text revision.

References

[1] 1Password, "About the 1password security model." https://support.1password.com/1password-security/, 2022. Online; Accessed 25 November 2022.

3 Analytical Memo

TO: All SCSNY Staff
FROM: Michael Garcia, IT
DATE: November 25, 2022
SUBJECT: Password Manager

With the ever increasing amount of technology related services that Sunnyside Community Services accumulates, the IT department has determined has determined that there is an inherent risk that these services bring. The risk is the widespread use of password reuse throughout these services. To remediate the issue of password reuse, IT department is mandating that all faculty to use a password manager. The password manager will be provided to all faculty beginning December of 2022.

Why password reuse is bad

Troy Hunt, a renowned information security researcher based in Australia, has testified in front of congress the inherent risks that we have in our cyberspace. He discusses the rampant data breaches that occur and how password reuse contributes to fraud and identity theft [1]. Moreover, NASDAQ reported that there were 1,862 breaches in 2021, with 294 million people impacted [2]. In conclusion, do not reuse your passwords.

Using a password manager

Using a password manager, we reduce the likelihood of password reuse therefore lessening the impact of a data breach within our organization. When the service is rolled out, we will provide support to manage this new tool. Additionally, our future security audit (this will be a surprise!) will be on the lookout for any written password post-it notes on your desks, so please be diligent with our security hygiene.

Many thanks,
Michael Garcia
IT | Information Security Team

References

[1] T. Hunt, “Here’s What I’m Telling US Congress about Data Breaches.” https://www.troyhunt.com/heres-what-im-telling-us-congress-about-data-breaches, 2017. Online; Accessed 25 November 2022.

[2] C. Morris, “After a Decline in 2020, Data Breaches Soar in 2021.” https://www.nasdaq.com/articles/after-a-decline-in-2020-data-breaches-soar-in-2021, 2022. Online; Accessed 25 November 2022.

4 Op-ed Article

The Government Can't Keep You Safe Because They Don't Understand Technology

Michael Garcia

November 28, 2022

Figure 1: Equifax CEO Richard Smith appears before Congress, where he answered questions about the Equifax breach.

Would you happen to know that there were 1,862 reported cybersecurity breaches in 2021, with more than half of those figures having been leaked with Social Security numbers and their respective names? You may at first assume you were not impacted by the breach. However, if you've applied for any type of loan, housing, or credit line, you have already been impacted. In 2017, Equifax, one of the three largest credit reporting bureaus in the United States was impacted by a cyber attack. The breach leaked first and last names, Social Security numbers, birth dates, addresses and driver's license numbers of 143 million Americans [1]. These types of information are an accessory to stealing identities which could lead to fraudulent financial activity under your name without you knowing for years, once it is too late.

Corporations that fail to uphold their integrity often face little to no substantial repercussions with heavy consequences for their users [2]. The United States government has failed to protect its citizens' confidentiality against an ever growing lack of care in the implementation of technology. I find this important because victims that have been affected by these cyber attacks are often left to fend for themselves, resorting to solutions that have ongoing costs. These solutions include credit monitoring services, password managers, and ad blockers; these tools often require the user to understand how to utilize them effectively. Having worked at an organization that facilitates many non-technical individuals, I personally find it hard to believe that victims of cyber attacks will even know how to take the first steps to defend themselves from attacks.

These breaches happen often because of a variety of factors that usually fall under the umbrella of technology and user behavior. Technology could include, but not limited to, the website you use, the applications that are used to run the website, and the physical devices that run the data to serve the needs of the user. On the other hand, user behaviors as the name implies, are the actions we perform to interact with technology. These could be responding to an email, clicking an ad, or visiting a website. The use cases or behavior I mentioned may seem innocuous however, these properties are the same surfaces that a hacker can exploit to initiate an attack.

These attack surfaces are often mitigated by proper security implemented by the organization responsible for the service. Websites you visit are often encrypted so it can't be intercepted; applications are tested rigorously many times to determine if there is a risk of it being exploited. Furthermore, malicious emails are filtered through by means of effective spam systems designed to catch phishing emails (emails that try to steal your identity by pretending to be a legitimate entity) [3]. But as businesses go, there are times where cost cutting takes effect and cybersecurity is usually the first one to go [4]. It is often difficult to justify cybersecurity costs because they don't show return of investment well. For example, we could frame that no cybersecurity incidents occurred in the organization this year as a sign of a well implemented system or a system that does not need further investment. In the chance that a cybersecurity incident does occur, the total loss for an organization dwarfs the cost of investing in proper cybersecurity [5]. Furthermore, the loss of trust and reputation is incalculable.

These organizations continue to have shortcomings because the United States government does not utilize a proper framework to secure our infrastructures [6]. Over the past few years, the United States has only begun to build up our cybersecurity frameworks to help organizations. In 2014, the National Institute of Standards and Technology released the Cybersecurity Framework aimed to help organizations assess the risks they face [7]. In 2018, former President Donald Trump signed into law the establishment of the Cybersecurity and Infrastructure Security Agency (CISA) that aims to protect multiple levels of the government against cyber attacks [8]. These few aforementioned milestones of framework and agencies are the reactionary answers to the growing cybersecurity problem we are facing in the United States.

Although we are slowly creating frameworks to help organizations become secure, there are two vital problems that I believe continue to linger. To begin with, large organizations that are not actively investing enough into their cybersecurity and do not face consequences large enough so that that they are deterred from reducing their cybersecurity investments. Second, and most importantly, the legislative body does not have a firm grasp on how technology works. Our legislatures need to understand the impacts and operations of technology in our modern world in order for them to create laws and frameworks [9]. We need to vote-in legislatures that bring both logic and an open-mindedness to learn so we may quickly implement proper frameworks to secure our technology.

When the proper legislature is amended, we can hope to see a much more secure cyberspace. In the European Union, they have already seen compliance by large corporations due to the General Data Protection Regulation (GDPR). This piece of legislation enforces organizations to properly process and secure data [10], otherwise they would face large fines [11]. One could comfortably assume that once this form of legislation is proposed in the United States, we will have better protections as netizens of the United States.

References

[1] L. Mathews, "Equifax data breach impacts 143 million americans," Nov 2019.

[2] L. H. Newman, "$700 million equifax fine is still too little, too late," Jul 2019.

[3] K. Jansson and R. von Solms, "Phishing for phishing awareness," *Behaviour & Information Technology*, vol. 32, no. 6, pp. 584–593, 2013.

[4] S. Duca, "Treat cybersecurity as a strategic investment, not a sunk cost," Dec 2021.

[5] A. Bernard, T. Staff, A. Abdullahi, M. Shacklett, and B. Stone, "Cybersecurity prevention can save your company $682k," Apr 2020.

[6] I. T. R. Center.

[7] H. Moss, "Achieving successful outcomes with the nist cybersecurity framework," Feb 2019.

[8] C. Cimpanu, "Trump signs bill that creates the cybersecurity and infrastructure security agency," Nov 2018.

[9] C. Kang, "Congress, far from 'a series of tubes,' is still nowhere near reining in tech," Dec 2021.

[10] "2018 reform of eu data protection rules."

[11] "30 biggest gdpr fines to-date: Latest gdpr fines: Updated 2022," May 2022.

5 Initial Working Drafts

Getting Started with 1Password Password Manager

New User Guide | Version 1.0

Author: Michael Garcia

Contents

Kim Liao: nice organizational structure and formatting!

Introduction

1Password is a password manager designed to help you manage all your logins, private keys, and credentials all in a secure application. 1Password stores all your information in a virtual vault that is encrypted behind a PBKDF2 key-derivation algorithm. This means that your information's encryption will be difficult to brute force open by attackers.

Kim Liao: remember that your audience is a layperson -- imagine a grandma, or a non-techie user. Why is this password manager going to help them keep their CC #s and private data secure? What's the difference between a login, private key, and credential? What is a virtual vault, and why is this key-driven algorithm trustworthy?

To keep your information secure, we limit our knowledge of any sensitive user credentials. This includes your master password, your secret key, and information stored in your vault. Your master password is something you know, this is the only password you'll have to know, we'll remember the rest. The secret key is something you have, this is a 34-character key that is unique to you, store this key somewhere physically secure such as a safety deposit box or safe.

Kim Liao: which info is known by the company, and which is shielded from them?

Kim Liao: this is great!! Very clear. This level of detail is perfect

Getting Started

1. Signup with 1Password
   https://1password.com/sign-up/

   You'll get an email to confirm your account. Then you can choose a strong account password, which you'll use to unlock 1Password.
2. Download 1Password to your devices
   https://1password.com/downloads/

   We support the following environments:

3. Add your logins and make your passwords stronger.

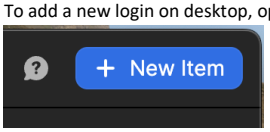
Kim Liao: what's the key? How is that different from the master password? Is the key something needed in case the user forgets their password? What's the ultimate purpose of the Introduction section in terms of informing or helping the user know what's going on with a password manager?

Kim Liao: is this the master password?

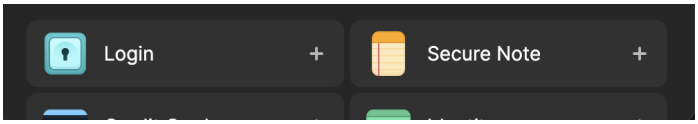
Kim Liao: what does this mean?

New Login Example

1. To add a new login on desktop, open the 1Password app and click on “New Item”.

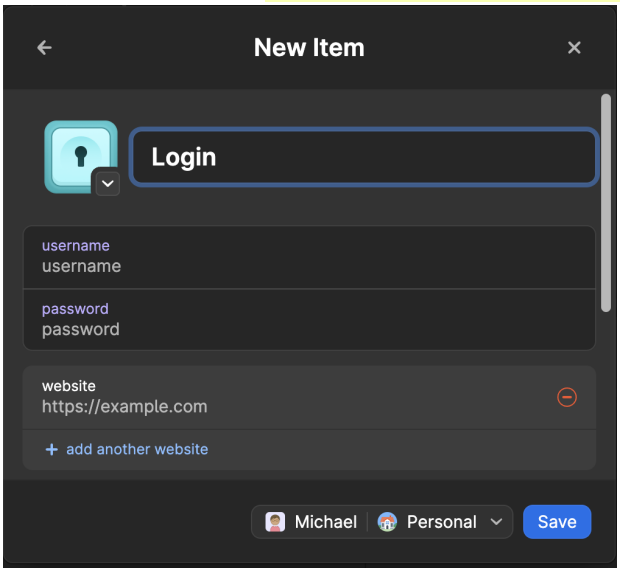


2. A new window will show, click on “Login”.



3. Another new window will show, fill in the details of your login, and then click save.

Kim Liao: so the user starts off knowing all of their logins? Then, does the password manager improve the complexity of different passwords?



FAQ

How does 1Password work, and why should I be using it?

1Password allows you to create a single account password that secures all your other passwords. Then you can use strong, unique passwords for all your online accounts, which means a security breach on one website only affects that one site.

Kim Liao: so do you make up all of the passwords for the manager?

How secure is 1Password? Can I trust 1Password?
The 1Password Security Design White Paper explains exactly how your secrets are kept safe. It's a lot to read, but it covers all the inner working 1Password if you want to learn more. 1Password is also SOC 2 type 2 certified, which is an auditing process that ensures 1Password securely manages data to protect your interests and privacy.

Would it be safe to store all my credentials under one umbrella?
Your 1Password account is kept behind a secure encryption. Your password and secret key together make it computationally infeasible to decrypt your information without the proper keys. Therefore, it is important that you keep your password and secret key secure and known only to you.

Can 1Password create passwords for me?
Yes, 1Password can create strong passwords that is unique to every account. All your accounts should have a unique password, 1Password makes that easy.

Do I have to fill in my logins every time?
No, 1Password has an autofill feature that can fill in logins for you inside apps or websites.

Can I still login if I forget my password and secret key?
If you forget your password or secret key, we would be unable to recover your account. It's important to keep the backup of your secret key somewhere safe and secure. Your master password should also be stowed away somewhere safe.

Revision History

Revision Date	Version	Name	Changes
10/16/2022	*Version 1.0*	Michael Garcia	- Initial Draft

Kim Liao: add citations here in brackets and put references at the end (hyperlinks are not customarily or necessarily used in IEEE, but in a lot of documentation it's fine. I'd just add the reference #)

Kim Liao: are

Kim Liao: great explanation!

Kim Liao: so what does someone do in the event of losing one or the other? What happens in real life when this occurs?

Kim Liao: also, one more question: can password managers go across devices, or be accessed from both phones and computers, etc?

Kim Liao: nice

Michael,
Great job on this draft!! Your organization is terrific, and your overall purpose with this document to inform the user of how and why to use a password manager is wonderfully effective.

As you revise, consult some of my margin comments above: in particular, explaining concepts and simplifying the language in the intro, as well as addressing a few logistics in the step-by-step installation instructions. Also, when you have sources to cite, please add a [1] bracket for an in-text citation and a References list at the end.

Great job, and can't wait to see how your Module 2 texts evolve!

TO: All CUNY Staff & Faculty
FROM: Michael Garcia, IT
DATE: October 23, 2022
SUBJECT: Excessive Password Reuse

With the ever increasing amount of technology related services that CUNY accumulates, the CUNY Computing & Information Services (CIS) has determined that there is an inherent risk that these services bring. The risk is the widespread use of password reuse throughout these services. To remediate the issue of password reuse, CUNY CIS is mandating that all faculty to use a password manager. The password manager will be provided to all faculty beginning December of 2022.

Kim Liao: why is password reuse so risky? Also, if this memo could address the resistance of older faculty (or less tech savvy faculty) to trusting a password manager, that could be even more impactful!

Reducing Security Risks

Password reuse is dangerous to one's professional and personal digital assets. For example, by a peer-reviewed study, it was determined that users are highly likely to create passwords that are the same or similar for what they use in other services. In order to protect the CUNY IT environment, we are mandating that different passwords are used and stored in a password manager.

Kim Liao: use a specific ## or % statistic, and note what the risk increase is -- or is it just that the stakes are much higher if you do get hacked?

We explored other options such as Single-Sign On (SSO) as a method to reduce password reuse. SSO allows users to use a single credential to login into multiple services. We determined it was also best to use SSO but since some infrastructure or services cannot be tied to the SSO we came to the conclusion that a password manager is required to make sure the infrastructure or services that do not support SSO are still secure.

Kim Liao: I liked your reflection in the blog post about SSO -- also, this is what John Jay currently uses. Does a password manager coincide with an SSO? (esp because we need to change passwords all the time!!) Which infrastructure or services can't be tied to SSOs?

By using a password manager we reduce the risk of password reuse and allow users to retain knowledge of their passwords. This will also increase our physical security as scribbled post-it notes should become obsolete.

Kim Liao: this is me!! OMG lol

Kim Liao: what are statistics, research, or evidence about the efficacy of a password manager? How do you propose getting everyone on board? Training faculty, offering stats of what works, or why they should trust it?

Kim Liao: you can trim this down

Many thanks,
The CUNY Computer & Information Services Dept.
CIS | Information Security
395 Hudson Street | 6th Floor
New York, NY 10014
security@cuny.edu

CIS Service Desk
646-664-2311
service.desk@cuny.edu

Michael,
Great job on this draft! Your structure, level of formality and diction is great, as is your focus on this audience and on rolling out a password manager at CUNY.
As you revise, I'd recommend digging deeper with research to give evidence as to the efficacy and trustworthiness of password managers, as well as to show what the risks are of reusing passwords. Amp up the evidence, and your claims will be even more persuasive!

The Responsibility of Account Security Has Been Transferred to Regular Users; That's a Problem

Michael Garcia

November 7, 2022

Security breaches has increased tremendously in tandem with the growth of our digital footprint. As more of our lives become entrenched in the inter-connected world, the small fragments of our digital profiles become krill for hacking whales. Negligence of companies, webmasters, and data brokers are pushing the responsibility of user security to the user themselves. Granted, users should be creating strong passwords and enabling multi-factor authentication, however companies often fail to protect their users such as Equifax [1]. We will go over how password managers can protect you by allowing you to manage your digital identities.

How Password Managers Can Protect Me

Password managers provide a secure and easy way for users to manage their credentials. These credentials could include online accounts, bank information, social security, any information that could be transcribed to text can be stored in a password manager [2]. Your credentials are secured behind a heavily encrypted file that only the person who knows all the details, hopefully you and you only, can open.

The encryption scheme the file goes through requires that the user has something they know and something they have. Something the user knows is a password, this is usually marketed by password managers as a "master password". The master password is ideally the only password you should remember; clearly this should also be the strongest password you can remember. Complementing this is something you have, which is usually a long and complex "secret key" that the password manager generates for you. One could assume that the secret key is a second password, but this password is extremely complex and unique such that a computer or a person would have a difficult time breaking. The password manager will only ask you for this secret key once to authenticate that the user attempting to open the encrypted file is you. After the first login, the secret key is securely stored on the computer so that the owner only needs to type their password every time they need

Kim Liao: this is a great point! Could make it more emphatically, such as "We Are Not All Cybersecurity Experts," or "Policing Your Own Data" or something much pithier than what I can come up with on the fly!

Kim Liao: "hacking whales" is an excellent analogy!!! Also, this idea that every password we make (no matter how innocuous) could leave us vulnerable to a cyberattack or identity theft is a great point. I would even start with that second, more impactful sentence! (and trim out the first one)

Kim Liao: great point!!!!

Kim Liao: rather than being a "How to" for a user (more of the goal and purpose of the Info Text), could you instead make a larger point about the ramifications??? Kim Liao: If we are all stewards of our own data, should Apple build a password into future iPhones? (I would pay for that!!! rather than have to sleuth out my own) OR should the government regulate or supply subsidized Password Managers? Or do consumers need to get more savvy right away, and invest in password managers like the new smoke detector or home alarm system, etc?

Kim Liao: nice evidence

Kim Liao: this is very informative, but not very persuasive. I'm still not totally sure yet what your ultimate argument is. People should use them? Anything else? Why does this changing digital

to access their password manager. If you're handing down the computer to someone else, you could simply de-authorize the key stored on the computer.

Of course, if you lose your master password or secret-key, you'll forever be locked out of your password manager. Reaching out to the company that develops the password manager to help you recover the account will only land you nowhere as they have zero knowledge of your password or secret key. Word to the wise, keep your master password and secret-key stored somewhere safe and secure, physically.

Demystifying myths

You would find that some people may have reservations with password managers. They often state that password managers can be a single point of failure. While this may be true in theory, in practice it is highly unlikely. As you have learned in the previous section of this article how password managers work; well, in a extremely high level overview. For a hacker to compromise your password manager they would have to be in possession of your secret key and master password. So unless you are a target for nation state hackers, you would be amiss of spy activities around your household.

Well then, one might ask, what if the developer of the password manager snoops on my accounts. Which is a valid argument, but many of the popular password managers ride on their reputation and regularly publish audits. The lifeline of a password manager is its reputation, which if ever tarnished, can bring down their customer base. Furthermore, password managers regularly go through internal and third-party audit which is hired by the company themselves or performed as a hobby by ethical hackers and security researchers. For example, a renowned security consultant that hosts HaveIBeenPwned.com, a database helping others find out if their account has been compromised, highly advocates the use of password managers [3].

Well, perhaps you might think password managers add steps or complexity. If anything, password managers reduce steps or complexity. Have you ever had a situation where you forgot, misplaced, or confused your password? A password manager can solve that issue by automatically filling out forms, which is more secure because it prevents you from entering credentials on a phishing site. You also don't have to rummage through your email looking for the "Reset Password" link every time you forget your password. Furthermore, if you use the same or similar password for every account you have, you are running the risk of credential stuffing. Credential stuffing is a form of cyberattack in which they attempt to login to other websites using credentials they found in websites they have hacked into. Password managers can solve this by having an extremely different password for every account and storing them for you, relieving you of the duty of remembering them.

You convinced me, but there are so many Password Managers, which one do I pick?

There are a handful of choices when it comes to password managers; 1Password, BitWarden, DashLane, and LastPass just to name a few. All programs have their own personality that you as a user might like in terms of user experience. At the root of their purpose and utility, they somewhat operate to the same degree. Whichever one you choose, it will be easy enough to perform due diligence with a simple Google search looking back at their track record, current offering, and pricing. There is one notorious password manager in the bunch that has a dodgy track record, which is LastPass [4]. LastPass has had multiple breaches over the years, yet the security of their encrypted file is prevailing. LastPass may be struggling with their reputation, but other vendors have proven their resiliency with a solid track record.

landscape matter to our society?

Kim Liao: are there any examples of this happening?????? Sounds intense

Kim Liao: could you perhaps frame this to be about how the "Myths around Password Managers are Making People Targets for Hacking?" Some of this language would be GREAT in your Info Text, if you want to move it and then make more argumentative claims in your Op-Ed Revision

Kim Liao: so is the issue that people believe these damaging myths, and don't protect themselves?

Kim Liao: this is very helpful! Thank you! I think I'll set up a Password Manager over winter break, LOL

Michael,
There's a lot of really wonderful writing in here, and so I applaud you for being so clear, informative, and specific about de-bunking myths and recommending reputable password managers to consumers.
My only question as an Op-Ed reader is why does this matter, and what are the repercussions for society? So if we are now tasked with protecting ourselves, should the government, our device makers, or our employers be obligated to help us stay safe? Does everyone need a Password Manager, much like getting car insurance or having smoke detector in our homes? Get a bit more argumentative and show us why it matters, and you're all set!

References

[1] T. S. Bernard, T. Hsu, N. Perlroth, and R. Lieber, "Equifax says cyberattack may have affected 143 million in the U.S.," *The New York Times*, 2017. Last accessed 5 November 2022.

[2] R. Price, "Password managers are an essential way to protect yourself from hackers — here's how they work," *Business Insider*, 2017. Last accessed 5 November 2022.

[3] T. Hunt, "Password managers don't have to be perfect, they just have to be better than not having one," *Troy Hunt*, 2017. Last accessed 5 November 2022.

[4] Wikipedia contributors, "Lastpass — Wikipedia, the free encyclopedia," 2022. Last accessed 7 November 2022.