Software has become an ever-increasing part of our day to day lives, and as technology advances and grows more complex, so do the threats of cybersecurity attacks against all types of users. While many of these cyber-attacks can vary anywhere from stealing your personal email to committing identity theft, one of the most prominent (and ancillary) forms of cyber-attacks is a compromised online account. Many companies are aware of this threat and do their best to encrypt user data and keep their databases secure, but nonetheless there is a common point of failure amongst all these systems that is extremely difficult to address: user passwords. Because users oversee creating their own passwords, and it is virtually impossible to explicitly force someone to create a strong password and change it often, many users adopt the common practice of designing weak passwords and reusing them across multiple different accounts and services. This isn't just an issue with non-technical users, either; from personal experience I can recall multiple instances of software engineers, those who are designed to create these very systems and ensure their safety, engaging in bad password practice, whether that be creating simple passwords, reusing them between various applications, or even storing all their passwords in a single, unprotected location. Needless to say, password hygiene is a very important part of having a digital presence, and as such it should be taken very seriously—so then why is it not?

Password managers have been in development since the late nineties to address this very issue of bad password hygiene. Using a password manager makes it extremely easy for users to generate complex passwords, avoid password reuse, and manage all these passwords without having to memorize each one individually. For example, a popular password manager, Bitwarden, has an extension for all popular web browsers. After creating or signing into your Bitwarden account, all the user must do is come across a page where they are either signing in or creating a new account. In the case of signing in, the user can easily click the Bitwarden icon in their navigation bar and autofill the relevant login credentials. In the case of generating an account, the user simply has to click the same icon, click "generate a new password", and the user will immediately be prompted with a highly complex and secure password that can be simply copied and pasted when creating an account. Given the simplicity of using this service, then, why is it that more people don't adopt password managers or better password practices in general when browsing the web? And more importantly, what is the best strategy to increase user adoption?

Many researchers have taken to figure out why exactly it is that many people don't use password managers despite their importance and ease of use. These studies primarily rely on surveys to collect their data, and they often include both users and non-users of password managers to try to figure out what best incentivizes good password habits and how businesses can use these findings to increase user adoption. While there are many differing opinions on what the best strategy is to increase user adoption, researchers generally agree that non-users (i.e., people that don't use password managers) share a couple of common reasons as to why they don't engage with password managers. The biggest reason as to why non-users do not engage with password managers is due to a lack of understanding of how the technology works. Unfortunately, while password managers are strongly encouraged to almost every single online user, there is very little done in the ways of educating the user on why exactly the password manager is safe and some of the technology behind its robustness.

When discussing the topic of password managers, individuals usually talk about how it helps the end user and their own lives, but there is rarely any discussion about the security of the application. Why should users trust a password manager with all their passwords? After all, common sense tells you not to put all your eggs in one basket, and to instead diversify in order to minimize risk. While this concept does have some merit in certain contexts, it is largely misinterpreted by the common user. With relation to the stock market, for example, keeping track of complex, lengthy passwords individually is akin to putting your money into individual stocks. Each individual company must be researched before purchasing the stock, the investor must keep tabs on each company to either buy/sell shares from time to time, and all in all it becomes a huge headache for the average investor to keep track of. On the other side of the spectrum is an ETF, a single investment that maintains the diversity of multiple stocks while at the same time offering a safer return and minimizing the need to keep track of several companies at once. Despite this analogy, many are suspicious of how secure most password managers really are, and many users cite this as the primary reason that they do not engage with password managers (Jamil). What's even more interesting, however, is that most password manager users share similar sentiments to non-users in their understanding of the technology.

This finding has led some researchers to conclude that one of the most effective ways to increase user adoption of password managers would be to increase the creation and distribution of educational resources that can help inform users about the robustness of password managers

and why they are safe (Mackie). However, other researchers have found that a big part of why password managers have such a low adoption rate is due to the fact that users lack the time or motivation to learn about password managers, and that they often feel inundated with information surrounding their use and how they work (Fagan). Given this sentiment that many non-users share, it then seems a bit perplexing that many users are afraid of what they do not fully understand, yet they also have no desire to put the time and effort into understanding those concepts. This makes sense given that humans are largely irrational creatures whose emotions play a big role in decision making (Fagan), but it nevertheless convolutes the idea of whether additional information about how password managers work would be effective in increasing user adoption.

Many users of password managers often report higher levels of technical ability and a younger demographic (Fagan), but despite this being in their favor, many do not use password managers because it keeps their passwords secure. Instead, many "users" report that they have many different online accounts and so their primary motivational factor is a fear of losing their accounts (Ramakrishna). Rather than having a moderate understanding of how password managers work and deciding to use the service in order to improve the safety of their passwords, many users admitted to not fully understanding how a password manager works (Fagan). Instead, the two main reasons that users decide to adopt a password manager seem to be to easily keep track of multiple passwords and to avoid getting their accounts hacked. While all roads ultimately lead to Rome, it is interesting to observe that a fear of losing online accounts is much more effective in influencing individuals than the desire to follow good security practices.

It follows, then, that several researchers have concluded that messages about security threats and compromised passwords may be effective in increasing password manager adoption, as the subtle use of a fear tactic is commonly effective in persuading individuals to action (Ramakrishna). However, other researchers have found that non-users often hold the self-perception that they don't have many online accounts and therefore do not need to concern themselves with compromised accounts and password hacks affecting their day to day lives (Fagan). If many of these non-users believe that their online activity is not frequent enough to worry about the impacts of accounts being compromised (i.e. a grandma who simply uses a single social media account), then it seems that messages regarding looming security threats would not be an effective motivator for many non-users who fall under this umbrella.

An alternative strategy that researchers came up with to promote better password practices in general was to provide users with more persuasive text when creating a new account and setting up a password, as highlighted in a study by Mackie. In this study, it was shown that providing users with helpful text that guided them on how to make a complex yet memorable password was very effective in causing users to adopt a strong password, especially in relation to the passwords created by users who encountered the traditional password creation suggestions (minimum length, one or more special characters, etc.) Users who engaged with this persuasive text even reported saying that the practice was fun for them to undertake, further highlighting that it is a method that may be easily adopted by users. Given the effectiveness of this strategy, some researchers like Mackie have concluded that better password practices should be encouraged directly to the user, as opposed to encouraging individuals to use password managers and have them generate the passwords. This conclusion takes a brand new approach at the issue of password manager adoption (which is desirable because it increases better password practices), and seems to be a bit more straightforward than convincing users to adopt password managers. However, it is also important to note that this study was conducted with people who actively knew they were participating in a research study, and so the results may not reflect the real-world behaviors of an individual.

A possible solution to addressing this issue of people not adopting the suggestions is to somehow force them to engage with the persuasive password text before generating the password, which may lead to the users following the suggested practice and developing a strong password. However, in the case that this specific solution does not work, some researchers have found an approach that may be more effective: educating the user. While many companies and organizations have traditionally tried their best to educate consumers about good password practices and why they are important, there is very little being done in the way of educating the user *while* they are generating a password for a new account. In these cases, it may be useful to address the common misbelief that the benefits of bad practices (such as sharing passwords with friends) outweigh the potential drawbacks, and to possibly increase the user's perceived risk of their account being hacked. However, several studies that have shown that many people don't even perceive any risk from the act of reusing passwords and not changing them (Burak), which

further complicates the idea of whether or not more persuasive text would help users adopt better password practices.

A final approach worth mentioning is the idea of making password managers easier to use. Despite the ease of use of applications like Bitwarden (which was discussed earlier), not all password managers are designed very intuitively for non-technical users. Some require knowledge of two-factor authentication to secure the account or require a roundabout method for generating and adding logins to the password manager. Given these shortcomings, many researchers have concluded that focusing on making password managers easier for non-technical users would be the most effective way to increase adoption, as it would help address a major concern that password managers are complex and require a time sink that many non-users cannot afford (Fagan). While this seems like an intuitive strategy at first glance, other researchers have found that the ease-of-use of a password manager actually negatively impacted user adoption (Ramakrishna). This is because many non-users believe that the complexity of a password manager is reflective of it security, meaning an easy to use password manager is perceived as insecure due to its simplicity. Due to this disparity between whether or not easy to use password managers would increase user adoption, researchers have not agreed that this is the most effective method for increasing user adoption of password managers.

All in all, there are a variety of factors that influence an individual's decision to engage or not engage in good password practices. While there is a bit of variance in terms of the demographics between the two parties, for the most part non-users seem to shy aware from tools like password managers due to a lack of understanding or a misbelief that they don't have enough accounts to warrant a password manager; on the other hand, users of password managers also cite a similar lack of understanding of password managers, and instead mostly engage in good password practices for their own convenience and to avoid having their accounts hacked. Although there is a decent amount of research that has been done to understand why exactly individuals make these decisions, there is a copious amount of inconclusive research as to what the most effective method is for increasing user adoption. This primarily stems from the issue that humans are emotional and irrational creatures, which makes it extremely difficult to find a solution that would appeal to a large majority of individuals. There is also still work to be done in terms of implementing these suggestions into public applications and then gathering data from those scenarios. Researchers have come up with various potential solutions to the issue of bad

password practices, but almost all studies have been limited by the fact that the data was gathered either from surveys or from designated research scenarios. It would be extremely insightful to have this suggestions implemented in a public application and to gather data from those scenarios, as those would be the most effective in reflecting what actually works and what doesn’t in the real world.