2022

Password Managers: Secure Passwords the Easy Way

Alexander Master
Purdue University, amaster@purdue.edu

Password Managers: Secure Passwords the Easy Way

Alexander Master

Center for Education and Research in Information Assurance and Security (CERIAS)
Purdue University, West Lafayette, IN, 47906 USA
amaster@purdue.edu

Abstract. Poor passwords are often the central problem identified when data breaches, ransomware attacks, and identity fraud cases occur. This Purdue Extension publication[1] provides everyday users of Internet websites and computer systems with tools and strategies to protect their online accounts. Securing information access with password managers can be convenient and often free of cost, on a variety of devices and platforms. "Do's and Don'ts" of password practices are highlighted, as well as the benefits of multi-factor authentication. The content is especially applicable for small businesses or non-profits, where employees often share access to systems or accounts.

1 The Problem With Passwords

People who routinely use technology know the frustration of creating username and password combinations for most devices and online services. Unfortunately, many users create short, predictable passwords for their accounts — or worse, they use the same password across many different websites, which can make it easier for criminals to access their information.

The FBI received more than 790,000 complaints of cybercrime in 2020 [1]. The Federal Trade Commission reported nearly 1.4 million cases of identity theft in the same year, which is almost double the amount reported in 2019 [2]. One of the ways criminals perpetrate these crimes is by taking over online accounts.

Suppose a large company experiences a data breach (thousands happen each year in the United States alone), and attackers publicly post customer login information. In that case, criminals can use the revealed password of a user to attempt to access that user's other accounts. Even if a user's password is different across accounts but uses a similar base with an added suffix or prefix, this significantly narrows down the number of guesses for a targeted attack on an individual. Criminals can also use "brute-force" techniques with software to guess passwords [3].

Despite these issues, most people do not follow good password practices (see Figure 6). If passwords are so crucial to securing our identities and transactions,

[1] This article has been published to the Purdue Education Store, and is freely available at `https://ag.purdue.edu/department/asec/ext-pub-ace15w.html`

why do many people struggle? To answer this question, it helps to understand what makes a strong password and the challenges users face in remembering so many passwords.

2 What Makes a Strong Password?

First, a password should be unique to each account a user owns. It is crucial to avoid password reuse because of the methods criminals use when attempting to access online accounts. Second, each unique password should be long enough to impose a high computational cost, making brute-force attack methods ineffective.

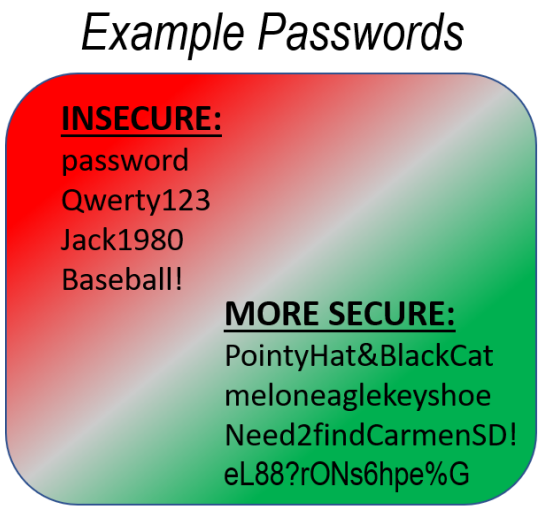

Fig. 1. Examples of insecure versus more secure passwords.

For example, a Tulane University calculator tool estimates a 15-character password, with two uppercase letters and 13 lowercase letters, would take more than 3.7 million years to try all possible combinations [4]. Fortunately, some online platforms limit the number of login attempts (within a short time period) to prevent some of these attacks. However, not all devices or websites do this, and password length remains an essential aspect of password security.

Third, users should avoid using a simple word (such as one found in a dictionary) as a password. Criminals use dictionary lists in some password attacks. Adding additional complexity (such as capital letters, numbers, or symbols) can help increase the strength of a password, although length is more important. A helpful strategy for making long passwords is combining random words (such as "orangeeaglekeyshoe") as shown in this Stanford University infographic explaining password complexity [5]. In general, a password is strong if it is long and random.

Unfortunately, users have many accounts to maintain across websites and devices. One research study estimated that an average user has one to seven unique passwords, but uses them on 10 to 50 online accounts [6]. This discrepancy is likely to continue to grow. It is difficult to remember so many passwords, especially when different sites have their own password format requirements.

Fortunately, there is a secure and convenient way to protect accounts with strong, unique passwords: Use a password manager.

3 A Solution: Password Managers

A password manager is software that uses encryption technology to make a virtual "notebook," or database. Users can store as many passwords as they like inside it. Encryption works by scrambling the contents of the database so that only the person who knows the key (the database password) can unscramble the content. In this way, the user must only remember one strong password to unlock the database. The software "remembers" all the rest.

Cybersecurity experts from the U.S. government (CISA) have recommended using password managers [7]. Researchers from Carnegie Mellon University and the U.S. Computer Emergency Readiness Team have stated that password managers are "one of the best ways to keep track of each unique password or passphrase that you have created for your various online accounts" [8]. Technology journalists have also weighed in on which password managers people should use [9].

There are many password managers available today. Some are free, some have a one-time cost, and others require a subscription service. Some run locally on your device, while others require an Internet connection to a company's servers to function. Password managers are available on many devices, such as computers, smartphones, and tablets.

In this publication, we will use KeePassXC as an example to show how to use a password manager. The steps described below can generally apply to any password manager you choose. This guide should not be considered an endorsement of a particular product or service by Purdue University. Ultimately, each individual or business must choose the software that best meets their needs.

4 KeepassXC

KeePassXC is a free password manager that can effectively help secure a user's online presence. The software is open-source, meaning the code is openly available for everyone to see. Anyone can make suggestions or contributions to improve the software — and many technology practitioners have had the chance to review the code to assess its functionality and security. If experts find bugs, they can easily and transparently report them. The KeePassXC team patches the software and releases new versions as needed. KeePassXC is one of many open-source programs available; it runs locally on your computer and does not require external servers or Internet connectivity to function.

To begin using KeePassXC, you can download the latest version from their site [10]. At the time of this writing, KeePassXC supports three major operating systems: Microsoft Windows, Apple macOS, and Linux. Follow the instructions on the KeePassXC website to download and install the appropriate version for your operating system.

The first time you run the software, you will select "Create new database." Follow the prompts by answering the questions. The default encryption settings should be sufficient for most users. When the software prompts you to enter a database password, ensure the password is strong and unique, because it protects all of your other passwords. Also, ensure the database password is one you will remember, because you cannot recover it if you forget it. Consider writing the database password and storing the paper in a locked location.

To get started, click the "+" (add a new entry) button, shown in Figure 2. Once you do, you will open up a new box that allows you to enter the information for an individual account (Figure 3). There are fields for "Title" (a name describing the account), "Username," "Password," "URL" (if it is a website login), and any additional "Notes" (PIN codes, security question answers, or any other relevant information).

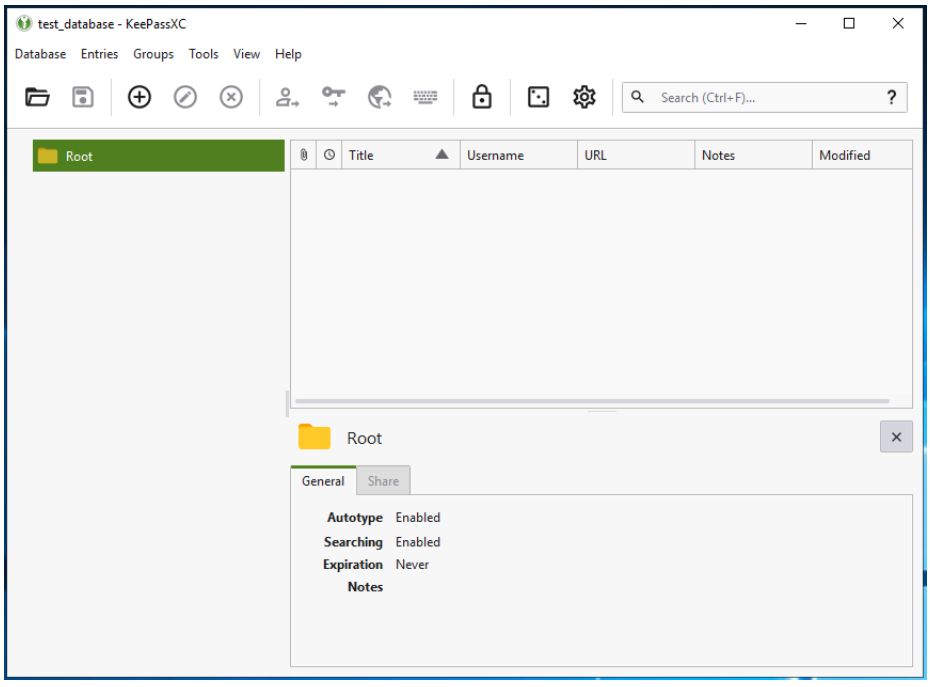

Fig. 2. An empty KeePassXC database.

Notice that anything you type in the password field is shielded from view by dots. If you press the eyeball icon next to the password field, you will see the password in plain text. Use this feature wisely; do not reveal passwords like this when someone could peer over your shoulder and view confidential information.

The software also includes a random password generator tool that can help you create new passwords. Access this tool by pressing the dice icon next to the password field (see Figure 3). This will open a new window to generate a random password (Figure 4). Select the parameters you prefer, such as password length and whether to include capital letters, lowercase letters, numbers, and special characters. When you are satisfied with an entry, click the OK button, and the main KeePassXC window will appear. All of your entries will appear in the main window. You can organize them into separate folders in the left pane under "Root," or you can keep them all in the same folder for ease of viewing.

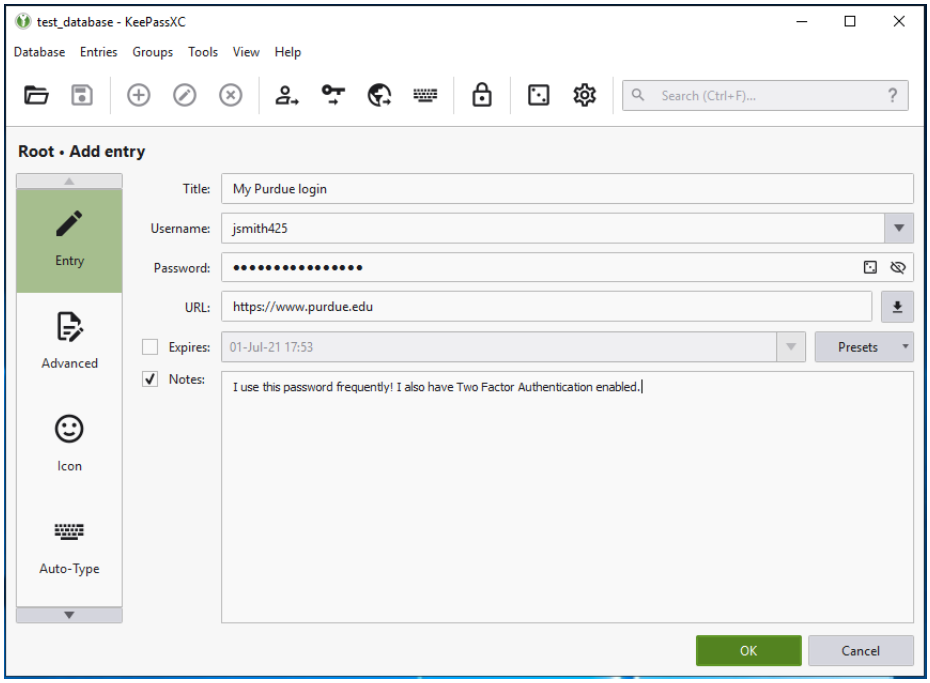

Fig. 3. A KeePassXC account entry window.

You can add all of your passwords for different devices and online accounts, or choose to leave some out. One approach to consider is not storing your primary email account password in the manager (and committing it to memory). Web services often will allow a password reset by email. Suppose your computer is stolen, or you are away from home and have an emergency that requires you to sign in to an account. In that case, you may still gain access by resetting the

password to a particular account by using your email. Just remember to update your password manager entry when you return.

An additional security precaution some people use when creating passwords is to add a memorized suffix to any randomly generated password. For example, let's say KeePassXC generated a random password of uL22!rkNs4hn#Y. When you actually log in to the site that uses this password, you paste that randomly generated password, but then add your suffix to the end — like "pluto" or whatever you choose. The final password the webpage requires is: uL22!rkNs4hn#Ypluto.

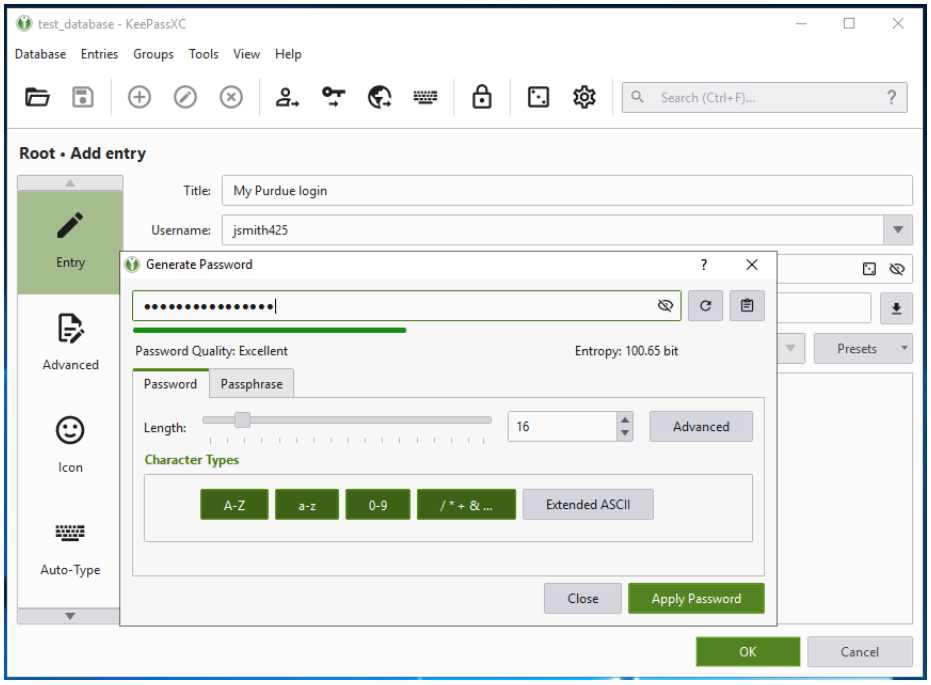

Fig. 4. The password generator window in KeePassXC.

The suffix trick could be helpful if your database were somehow compromised or taken by someone with access to your device — because of the suffix, attackers would not know the full actual password for the account. This precaution is not typically necessary, but may put some users' minds at ease.

5 Using Your Passwords

KeePassXC has multiple ways for users to input their passwords, especially for websites. You can right-click on an entry, select "Copy username" (or use the

keyboard shortcut Ctrl+B), and paste it into the username field on the website. Similarly, right-click on an entry, select "Copy password" (or use the keyboard shortcut Ctrl+C), and paste it into the password field. This way, your password is never revealed in plain view. In fact, if you randomly generated the password for an account, you may never actually know (or need to know) your actual password.

For a more advanced configuration, there are also browser extensions that can connect to your database. A browser extension is a piece of software you add to your web browser (like Firefox or Chrome) to give it enhanced functionality — in this case, the ability to securely populate a password from your database directly into a web page without the need to copy or paste. Password manager browser extensions still require the database password, but allow you to simply click on a username/password field on a website and fill in both fields.

Browser extensions create an encrypted connection between your database and the browser to provide the login information and do not store your passwords within the browser. Remember that these extensions are only for your convenience. Browser extensions are not necessary to securely store your passwords. You can find more information about the browser extensions available for KeePassXC on their "getting started" page [11].

You can use KeePassXC databases to store any confidential information. Suppose you wish to store locker combinations, safe opening instructions, or even smartphone/tablet passwords. In that case, you can simply use the eyeball icon to show the password within KeePassXC and enter it manually to the other device or lock. Any text you enter into the "Notes" section of a KeePassXC entry will also be encrypted along with all passwords. KeePassXC will show "Notes" in plain view while the database is open.

6 Securing Your Database

You should always take a few steps to secure your password database. First, we strongly advise that you occasionally back up your password database (Figure 5 shows a database file named test_database.kdbx). You can back up your database by copying the file to a USB flash drive, an external hard drive, or to a cloud storage website you trust. Creating backups of your database will protect you if your primary device is lost or stolen, or if you accidentally delete an entry and need to know what it contained.

Second, never store your password to the actual database on your computer along with your database — anyone who comes across your database password could access all of your other passwords.

Third, always make sure to use the latest version of the KeePassXC software (or any password management software you use). KeePassXC and many other applications allow you to enable reminders that inform you when new versions are published. You also can check the software website occasionally for new releases. The software will continue to function if you do not update, but may be missing security updates and new features as developers add them.

Fig. 5. An example database file labeled test_database.kdbx.

7 An Alternative Solution: Store Passwords on Smartphones

Some users do not work at a computer frequently or may prefer to store passwords on a mobile device. At the time of this writing, Android and Apple iOS are the most popular smartphone platforms. There are dozens of password managers in the Google Play Store and Apple App Store, as well as alternative app marketplaces. These password managers all have similar functionality, and the steps described above to set up a KeePassXC database will be similar for them as well. However, the application appearance will likely be different.

Like the computer options, there are free apps, paid apps, and apps that require a subscription. For example, Strongbox for iOS is open-source, has a free and paid option, can open a KeePassXC database file, and can operate locally on a phone without connecting to external servers. KeePassDX and Keepass2Android are similar options for Android phones. Always read about each app you are considering to ensure it will meet your needs and is regarded as secure.

8 Additional Considerations

Using strong, unique passwords across all of your accounts will help limit your exposure to cybercrime risk. If you do business with a company that is the victim of a data breach or ransomware attack, criminals may publicly expose your information that the company stored.

Many states have data breach notification laws requiring companies to disclose to affected parties (including customers) that they were victims of cybercrime [12]. If an organization informs you that your data may have been affected by cybercrime, log in to the affected account as soon as possible. Once there, change the password immediately. Also, check for any suspicious login activity or signs that your data has been changed. If you used that same password on other accounts, change the passwords for those other websites as well.

You can also proactively check if your account has been involved in a publicly known data breach. Websites such as haveibeenpwned.com and Firefox Monitor

allow you to enter your email address or phone number and then show you companies that have been hacked that included your personal data. If any results appear when you enter your information, make sure to log in and change the passwords to those sites. It may also be helpful to close the account if you no longer use the service.

If you purchase a device that has a default password set, always change it immediately. Devices such as Wi-Fi routers and smart thermostats commonly come with passwords such as "1234" or "cisco123." Criminal groups have extensive lists of these common manufacturer passwords and can use them to exploit your devices. Criminals can perform local attacks against Wi-Fi or Bluetooth-enabled devices. If a device is connected to the Internet, attackers can sometimes target the device from anywhere in the world. Even if that device has little personal information about you, it can serve as a starting point for compromising other computers or devices in your home or business if you leave them unsecured.

Finally, you should consider enabling multi-factor authentication (MFA) on all of your online accounts. MFA options vary by website, but all MFA options offer a second layer of protection for your accounts. If MFA is enabled, you will be asked to provide an additional piece of information after you log into your account with your username and password. Some MFAs send you an email to confirm your login, some require you to set up an authenticator app that generates a six-digit code that you must enter, others require that you enter a code you receive by text or phone. Let's say a criminal acquires your account password from a data breach and attempts to log in to your account. If MFA is enabled on that account, the criminal will unlikely have the means to provide the second piece of information required to log in, and their attack will fail.

9 Looking Toward the Future

In 2004 at an RSA Security Conference, Bill Gates (co-founder of Microsoft) predicted that password-based security would soon be a remnant of the past [13]. He outlined many problems surrounding password use and suggested that they "don't meet the challenge for anything you really want to secure." Unfortunately, 18 years after his remarks, passwords for web-based accounts are more prevalent than they have ever been. State governments in the U.S. relied on web accounts to offer vaccine and testing appointments during the COVID-19 pandemic, while schools had to use Internet resources to enable remote learning. Local governments and municipalities use websites to allow citizens to manage and pay for utilities. Online shopping has become the norm for many worldwide; the Adobe Digital Economy Index predicted that global e-commerce would amount to $4.2 trillion for 2021 [14]. Most of these platforms require usernames and passwords for authentication.

Many alternative solutions have been proposed, such as biometrics (fingerprints, facial recognition), smart card tokens, SecureID tokens, and one-time codes (from software or text messages). Many alternative authentication methods are available as a second form of identification - but websites generally require

a password by default, and the password is the primary way to log in. In September 2021, Microsoft began allowing their users to turn on a "passwordless" option for outlook.com email and Microsoft accounts. These initiatives give users more options for how they choose to secure their accounts. There may come a point when alternative login methods like these become the norm, and passwords are no longer the pervasive security challenge they are today. In the meantime, until a majority of online services provide alternate options for account authentication, individuals and businesses need a secure and accessible way to manage all of their passwords. Password managers make this task easy and eliminate most of the human error associated with password use.

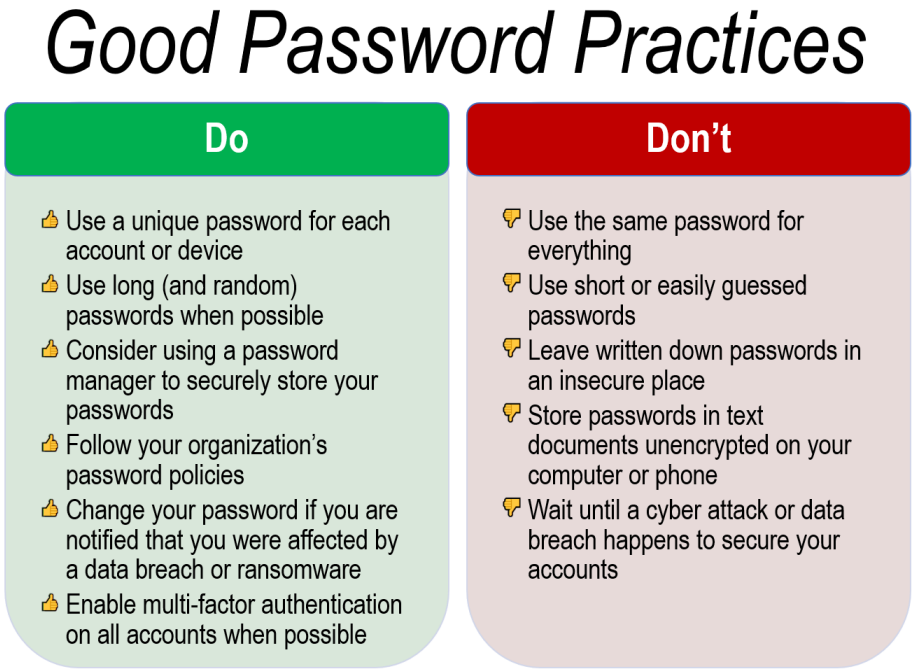

Fig. 6. Best practices for secure passwords

10 Summary

Technology is an ever-increasing aspect of our lives. People need secure passwords for their devices and web-based accounts to secure their identities and transactions. But it's difficult to remember many different sets of account credentials, so we often resort to using insecure or predictable passwords.

Password managers provide a software solution that empowers users to have secure passwords across their devices and accounts. Password managers signifi-

cantly reduce the burden of memorizing many passwords and can enhance the online experience [15]. You can reduce your risk of exposure to cybercrime if all your passwords are strong and unique to each account or device. With widespread adoption, password managers can help make the Internet a safer place for everyone's information.

Disclosures The author has not received compensation nor is affiliated in any way with products or services mentioned in this publication. Reference in this publication to any specific commercial product, process, or service, or the use of any trade, firm, or corporation name is for general informational purposes only and does not constitute an endorsement, recommendation, or certification of any kind by Purdue Extension. Individuals using such products assume responsibility for their use in accordance with the current directions of the manufacturer or provider.

Acknowledgements I want to thank Beth Forbes for shepherding this publication and encouraging me to publish my research. Your work in communicating science to the public is a vital resource to the state and to society at large.

I also want to extend my sincere gratitude to Dr. Christina Garman and Dr. James Lerums for their expert input and advice in the review of this publication. Your mentorship is greatly cherished.

References

1. 2020 Internet Crime Report. (2020). Retrieved June 21, 2021, from `https://www.ic3.gov/Media/PDF/AnnualReport/2020_IC3Report.pdf`.
2. New data shows FTC received 2. 2 million fraud reports from consumers in 2020. (February 4, 2021). Press Release, Federal Trade Commission. Retrieved June 21, 2021, from `https://www.ftc.gov/news-events/press-releases/2021/02/new-data-shows-ftc-received-2-2-million-fraud-reports-consumers`.
3. Hoffman, C. (July 6, 2013). Brute-Force Attacks Explained: How All Encryption is Vulnerable. How-To Geek. Retrieved June 21, 2021, from `https://www.howtogeek.com/166832/brute-force-attacks-explained-how-all-encryption-is-vulnerable`.
4. Brute force calculator. Retrieved July 2, 2021, from `https://tmedweb.tulane.edu/content_open/bfcalc.php`.
5. Password Requirements Quick Guide | University I.T. Retrieved July 12, 2021, from `https://uit.stanford.edu/service/accounts/passwords/quickguide`.
6. Gaw, S., & Felten, E. W. (2006). Password management strategies for online accounts. Proceedings of the Second Symposium on Usable Privacy and Security - SOUPS '06, 44. Retrieved July 12, 2021, from `https://doi.org/10.1145/1143120.1143127`.
7. Choosing and Protecting Passwords | Cybersecurity and Infrastructure Security Agency (CISA). (Updated November 18, 2019). Retrieved August 2, 2021, from `https://us-cert.cisa.gov/ncas/tips/ST04-002`.

8. Huth A., Orlando M., & Pesante L. (2012). Password Security, Protection, and Management. United States Computer Emergency Readiness Team. Retrieved August 2, 2021, from http://infragard-kc.org/InfraGard_KC_IMA_Website/Reference_Guides_&_Materials_files/US-CERT_Password_Security_Protection_and_Management.pdf.
9. Fowler, G. Your password has probably been stolen. Here's what to do about it. (July 12, 2018). Washington Post. Retrieved August 2, 2021, from https://www.washingtonpost.com/technology/2018/07/12/your-password-has-likely-been-stolen-heres-what-do-about-it.
10. KeePassXC Password Manager. Retrieved August 2, 2021, from https://keepassxc.org.
11. KeePassXC: Getting Started Guide. Retrieved August 2, 2021, from https://keepassxc.org/docs/KeePassXC_GettingStarted.html#_setup_browser_integration.
12. Data Breach Notification Laws by State | I.T. Governance USA. Retrieved August 2, 2021, from https://itgovernanceusa.com/data-breach-notification-laws.
13. Kotadia, M. (February 25, 2004). Gates predicts death of the password. CNET. Retrieved January 3, 2022, from https://www.cnet.com/tech/services-and-software/gates-predicts-death-of-the-password/.
14. Goolsbee, A., & Klenow, P. (2021). Adobe Digital Economy Index (ADEI) - Q1 2021. Adobe. Retrieved January 3, 2022, from https://business.adobe.com/resources/reports/adobe-digital-economic-index-april-2021.html.
15. Pearman, S., Zhang, S. A., Bauer, L., Christin, N., & Cranor, L. F. (2019). Why people (don't) use password managers effectively. Proceedings of the Fifteenth Symposium on Usable Privacy and Security (SOUPS). Retrieved August 2, 2021, from https://www.usenix.org/system/files/soups2019-pearman.pdf.