adafruit learning system

Protect Your Online Accounts with Strong Passwords & Password Managers

Created by nemesis0

Last updated on 2019-05-28 06:09:16 PM UTC

Overview

In this day, social media is everywhere. Checking trendy outfits on Instagram, retweeting cat videos on Twitter, or going to watch some fun tutorials on YouTube. It's impossible to not have social media.

But with all the fun, the importance of strong passwords is often overlooked. In a social experiment done by Kaspersky Lab, a cybersecurity firm, people were very quick to say the recipe used to cook up their passwords consisted of the following:

- Significant others name or year dated
- Names of: pet, grandma, mom name
- Sports team names or team players names
- Places visited

The main problem with the password quality the above data would generate is the password would be made up of *dictionary words,* meaning easy to understand words found in a dictionary. Examples of passwords would be `TommylovesJess2018`, `Iloveocko1234`, and `Gmama1954`.

The main reason people use simple dictionary-based passwords is that they rely on human memory to remember their passwords.

It is much easier to remember `Ilovecats1234` than `QdZKSKU5cH~<B[An`. However, in this day and age, it's time to make technology work in your favor. Using a password manager you can create complex passwords for each of your logins and never worry about having to remember them. In the following write up, we will examine some of the most used password managers and some of the cybersecurity attacks used to guess passwords.

Let's Talk About Account Takeovers

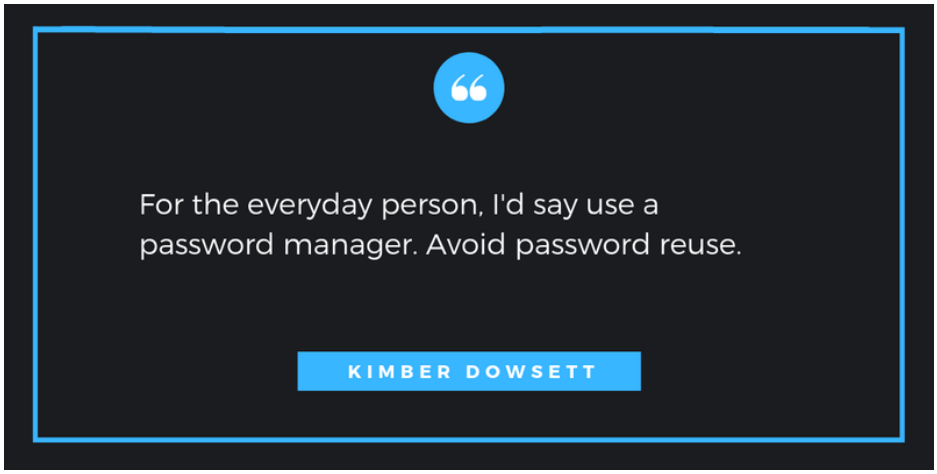
An account takeover is when an attacker has gained access to your personal account on a site or app. For the purpose of this tutorial, let's assume the takeover is due to someone knowing your login credentials. As the saying goes: *"Why hack it when you can just login."* There is a couple of ways someone can obtain your credentials some are:

- **Data Dump**, a massive list of user credentials posted after a company is hit with a data breach where user data is compromised. These lists often expose emails, passwords, and usernames.
- **Brute-Forcing**, forcefully trying to guess what your credentials are using either manual or automated tools online.
- **Social Engineering**, using physiological methods to deceive a person from knowing the true intentions of the

attacker. The attacker often is trying to extract data from the victim without being discovered.

We will explain the first two in more detail.

Data Dumps



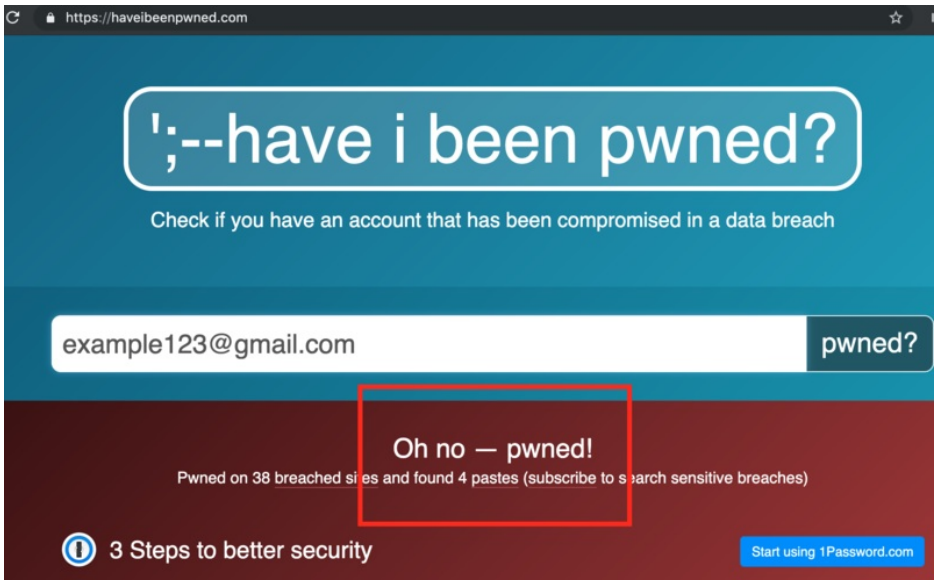
Data Dumps are usually large text files with user data from a breach an attacker dumped online or even at times, sells. The information is available to anyone looking for it. There are even sites such as cdn.databases.today (https://adafru.it/ET0) which collect user data and make available for security researchers to examine.

We will be examining a data dump from a Comcast data breach and explaining the pieces of data. A formatted snapshot down below, of an SQL query entry, gives us a quick understanding of the relationship of the data. The *INSERT INTO* notes the names of the columns of user data needed by the site. The *VALUES* are the data that is stored by the application from the user. So in the image below the **migration_password** for the user **kenny999991** is `damiano1`.

```
INSERT INTO `accounts`  (`account_id`,
                         `guid`,
                         `vanityname`,
                         `enabled`,
                         `suspended`,
                         `migration_status`,
                         `migrated`,
                         `migration_password`)
            VALUES
            ( (6202, '301220040111081131comcast.usrmig', 'kenny999991', 1, 0, 'A', 1, 'damiano1'),
              (6204, '229920040111082923comcast.usrmig', '1reef', 1, 0, 'A', 1, 'nolefan55'),
              (6208, '307720040111081207comcast.usrmig', '1remorgan', 1, 0, 'A', 1, 'le8bowsk5i'),
              (6209, '932020040606012940comcast.usrosp', 'kenny_davis', 1, 0, 'A', 1, 'hairLess1'),
              (6210, '266920040111081236comcast.usrmig', 'kenny_killa', 1, 0, 'A', 1, 'mnt_dew11'),
              (6212, '272820040111083213comcast.usrmig', '1renovation', 1, 0, 'A', 1, 'krystal1'),
```

While it can be scary to see other people's information leaked online, know the trouble will not stop there. If you are a high-value target, and your email and password from one site are known, chances are an attacker will input your credentials into other websites. If you *reuse the same password* then chances are other accounts of yours will be taken over.

There is a way to check if your email has been leaked online using the site called haveibeenpwned.com (https://adafru.it/ET1) which was created by Troy Hunt, who is now a Microsoft Regional Director and is also a strong web developer security advocate. If your email has been leaked online. then you will be shown which corporate breaches your information has been leaked, as displayed in the image below:

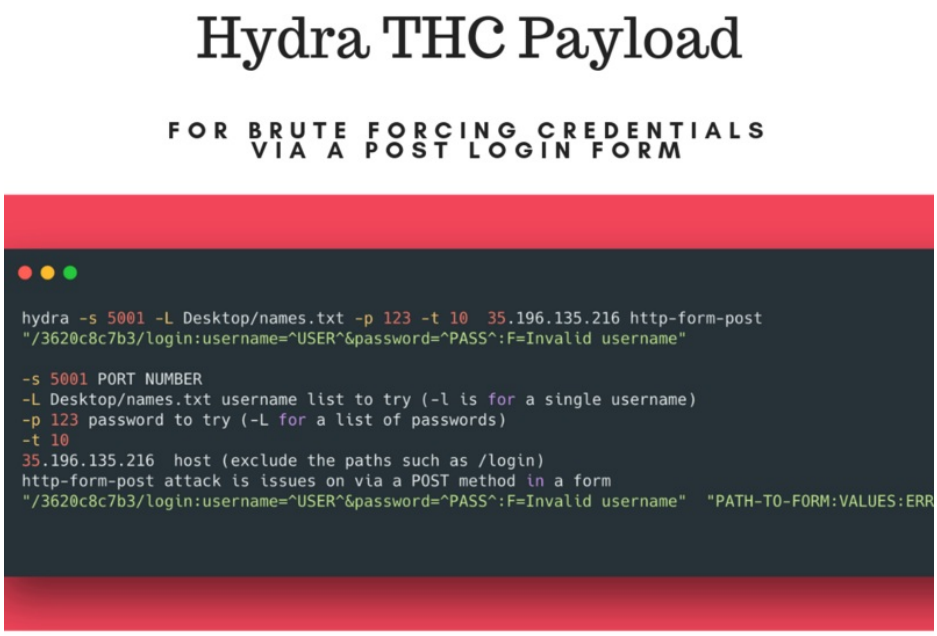


Some password managers such as **1password** automatically check with **haveibeenpwned** and alert you.

By far one of the most notorious threats to account takeovers is through brute-forcing credentials. Brute forcing is when an attacker will try to guess your password. And guessing is not complicated, given there are GitHub repositories such as Seclists. SecLists (https://adafru.it/ET2) is a compilation of the most used online passwords, usernames, directories available to the public for security researchers, CTF players, pentesters, and red teamers.

Pairing a massive compilation of default credentials from Seclists with a brute-forcing automation command line tool such as *Hydra* (https://adafru.it/ET3), an attacker can gain unauthorized access to your account.

The screenshot below shows how to use the command line tool Hydra to automate brute-forcing a login form:



What is a password manager and how they can help

As mentioned, using weak, easy to guess dictionary passwords such as `LionelMessi1960`, `HokageNaturo123`, `pusheenCat45` will not help protect your account from a potential account takeover. It also does not help your case if you *reuse* the same password on multiple services like Netflix, Instagram, and American Express.

What *will help* is having **strong** and **different** passwords for each site you use. The only problem with that is a password such as `@jSSb43jQmpf3&G%` is not very easy to remember.

But don't sweat it, because there is a tool that can not only generate long hard to guess passwords, but it can also store them for you. This tool is called a **password manager**.

What is a Password Manager

The main features of password managers have:

- They generate long hard to guess passwords
- They store the long passwords and usernames in a "vault" to autofill your login prompts
- They require that you have a master key to access your "vault"

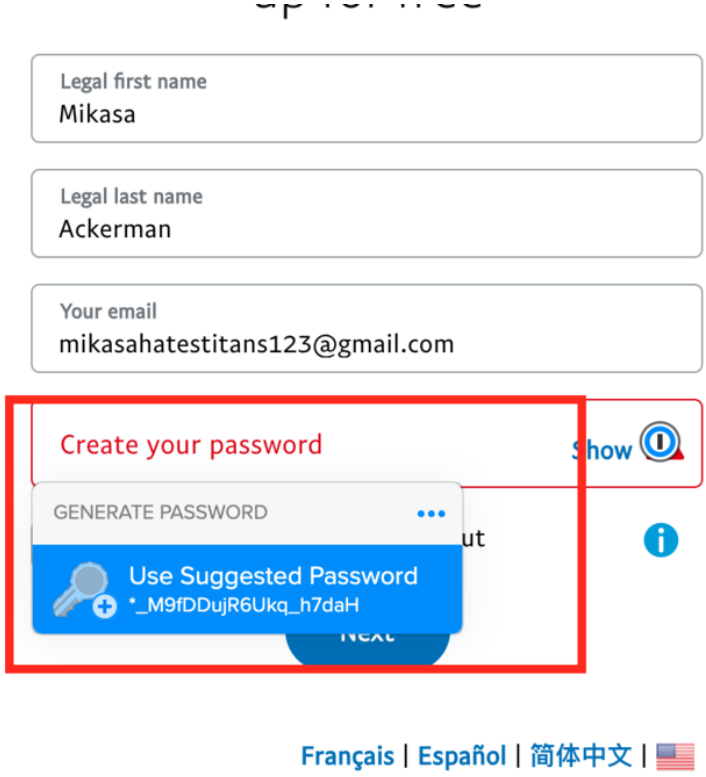
The whole point of password managers is to *manage* your passwords, so you do not have to. This means generating your password, storing them and granting you access to change the logins at any time. Which is a great solution to not have to reuse simple passwords on all your social, financial and medical accounts.

Password Managers: Features

A password manager can help when it comes to online password health by:

- Creating long hard-to-guess passwords on the fly
- Storing your passwords so you can automatically sign in

Take a look at the screenshot below, demonstrating how quickly it is to generate a password using a password manager. Right after the password is generated, a prompt asking to store the password will be immediately shown. This will store the password and next time the user logins into their account, the login will auto-populate. Yay for computers!



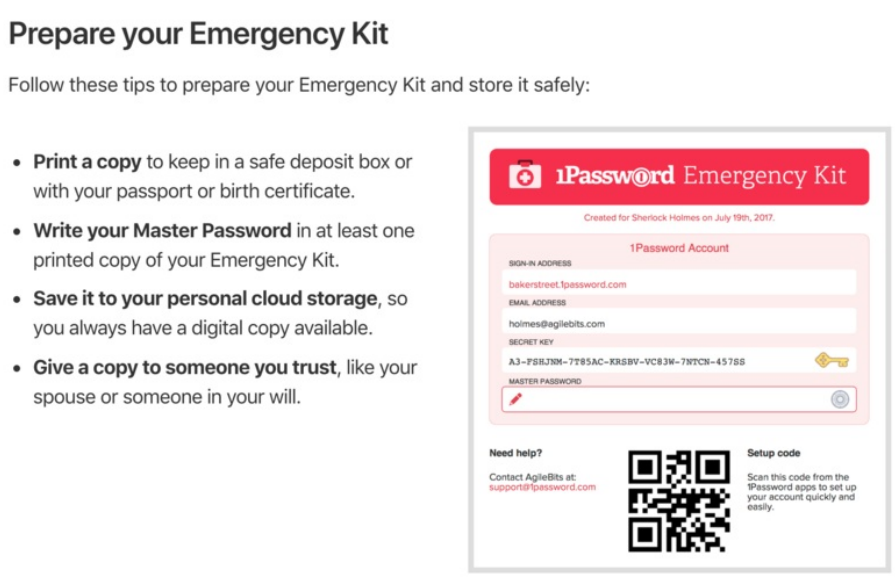
Password Managers: The Master Key to Rule Them All

The master key is the *mother* of all passwords. It's also a bit tricky to make, since, ironically, it's one you are recommended to remember, but it also needs to be secure. To better explain what to include in your master key, here is an excerpt from **Lastpass** (a password manager) on what they believe makes a great master key:

- Use a minimum of 12 characters, but the longer the better
- Use upper case, lower case, numeric, and special character values
- Make it pronounceable and memorable, but not easily guessed (e.g., a passphrase)
- Make sure that it is unique only to you
- Never use personal information
- A good example is: `Fidoate!my2woolsox`

Some password managers such as **1password** even provide an adorable emergency kit where you can prepare a PDF with your master key in case you cannot log into your account. What **1password** recommends you do with the PDF is to:

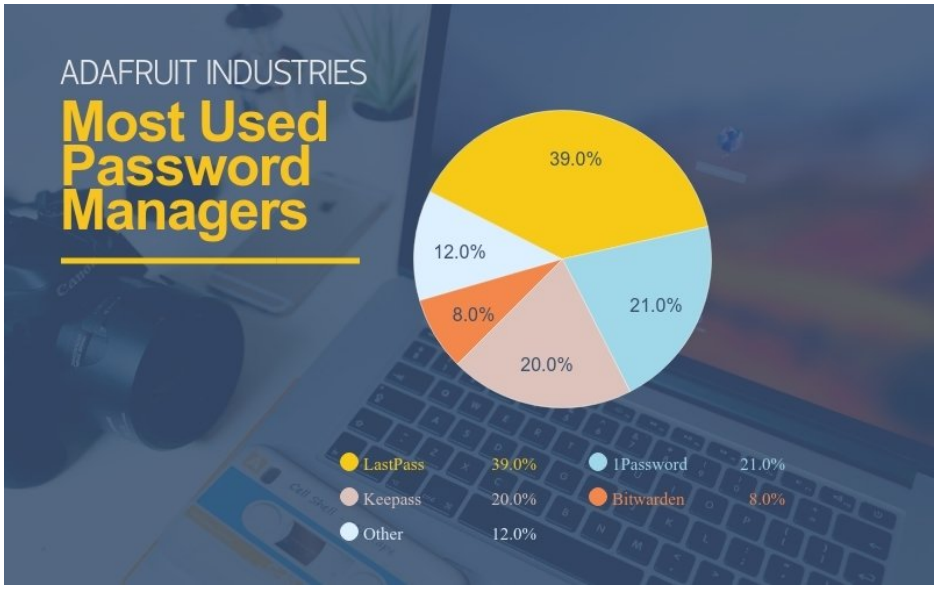
- **Print a copy to keep in a safe deposit box or with your passport or birth certificate.**
- **Write your Master Password** in at least one printed copy of your Emergency Kit.
- **Save it to your personal cloud storage**, so you always have a digital copy available.
- **Give a copy to someone you trust**, like your spouse or someone in your will.



Password Managers : Summary

Let's summarize the importance of password managers:

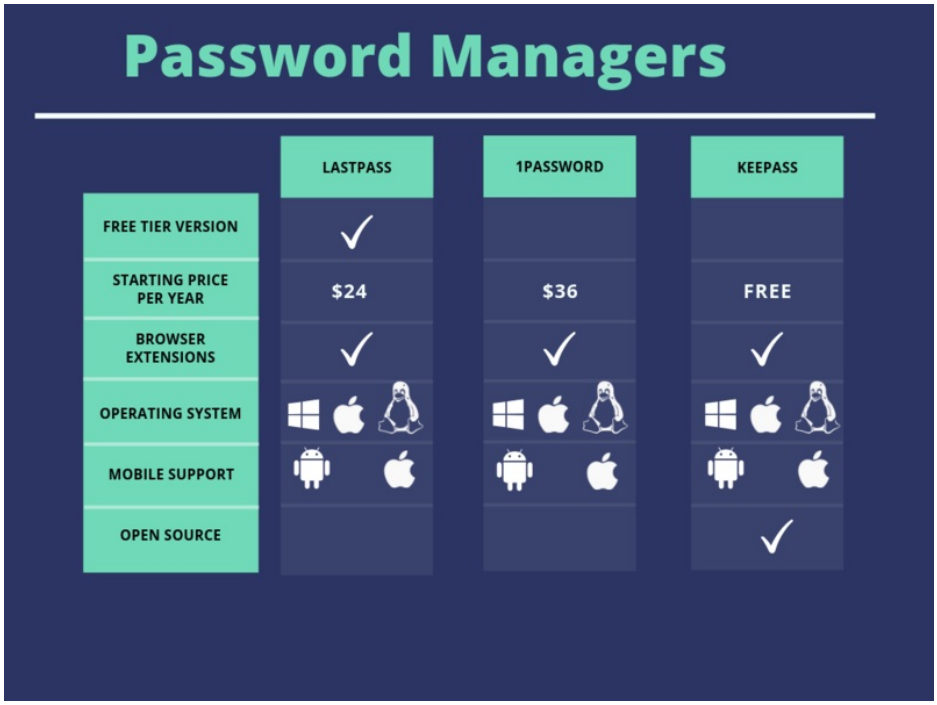
1. They can help create long passwords on the fly so you don't have to.
2. They store your long passwords and usernames to autofill the login prompts when you visit the sites
3. They all require you to memorize a master key which is the only key you will need to access your stored logins



Here at Adafruit, we want to offer the community as much information as possible so you can make your own informed decision about which password manager would be best suited for your needs.

We conducted a research questionaire and asked 100 people who were all either 1) Software Engineers 2) Working in cybersecurity, what their current password managers were and we recorded the answers in a pie chart shown above.

From the results, we decided to take a closer look at the top 3 password managers*, LastPass, 1password, and KeePass,* to see what they each had to offer. We recorded the results in the bar chart below.



The Top 3 Password Managers Results

LastPass

Lastpass was the top password manager with 39% of the users reported this as their current password manager. LastPass offers a free version of its services for the public to use. Lastpass is also around $24 annually for the 1 user account and prices increase when adding more members. Also, as a product, Lastpass mostly consists of a browser extension compatible with multiple browsers such as Chrome, Firefox, and Safari. Lastpass is also available on mobile for iOS, Android. A cloud storage solution of 1GB is offered to store your passwords as well.

1password

The second place password manager was 1password coming in at 21% usage. 1password only has paid versions and the individual plan is $36 dollars a year. Being the most expensive, 1password does not cheap out when it comes to features. Included with the annual fee, 1password includes a desktop app, browser extension, and mobile apps supporting all major platforms such as Mac OS X , Windows, Linux, Android and iOS. Also included is the ability to have your email cross-referenced with **haveibeenpwnd.com** checking if your data has been leaked from a data breach. Your data is also stored in the cloud up to 1GB and you are given options to backup the data to your favorite storage solutions such as iCloud, Dropbox etc.

KeePass

Almost tying the race with 1password, KeePass was the final password manager that made the cut to the top three. KeePass is also the only open source manager out of the top 3. It also has the most versions ranging from KeePass, Keepass2, KeepassDdroid, and Kypass along with many others. The full list is available at their official site keepass.info (https://adafru.it/ET4). All major operating systems such as Mac OS X, Windows, Linux, Android, and iOS are supported with corresponding KeePass versions. The password manager is a desktop application that pairs with a browser extension to manage all your login information. Keepass also requires a little more elbow grease to maintain. The credentials are stored in a local database on your machine which means you will have to back it up manually or install plugins to sync the database to your prefered storage method.

Wrap Up

With the information presented, we hope you pick a password manager that suits your needs and budget. Please use one!

Security is one of those things you want to be proactive rather than reactive about.