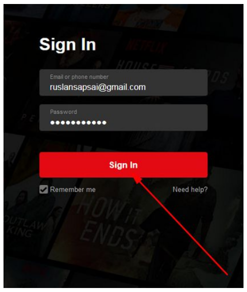
Manage Your Passwords
(or leave the front door open!)

Maryl Gearhart, Craig Griffith, and Hilary Naylor
with assistance from Sam Duncan

Ashby Village Technology Team

Ashby VILLAGE
Connecting People & Neighborhoods



Email or phone number: ruslansapsai@gmail.com
Password: ●●●●●●●●●●●

This article on passwords summarizes a June 2020 workshop co-sponsored by Ashby Village and the U.C. Berkeley Retirement Center. The topic of passwords was the logical follow-up to our previous February 2020 workshop on Internet Scams and Phishing. In that workshop, we highlighted strategies for minimizing the risk of becoming a scam or phishing victim:

- Use complex passwords, and different passwords for each account.
- Update regularly your operating system, browser, and apps.
- Back up regularly.
- Mark suspicious emails as junk/spam.
- Block pop-ups on browsers.

The focus of this article is the first recommendation - **strengthening passwords**. A strong password is essential, because the most common way that hackers break into accounts is by guessing passwords!

Why Are Passwords Important?

When you log in to a website, you are asked for both your username and your password. Your username - often your email address - is used to build a unique digital profile about you on that website. It is connected to information you have entered on that site, like your shipping address, credit card number, shopping history, financial transactions, or medical history.

You then enter a password to sign in. A simple or commonly used password makes it more likely that a hacker can gain access to an account, and commit financial fraud or identity theft. But creating a strong password AND remembering it can be difficult!

An Expert Shares Advice

We are fortunate that we have a local organization that can provide expert advice on online security and safety -- the Electronic Frontier Foundation. One of us interviewed a staff member, Bill Budington, to ask his advice on passwords -- on making, using, and managing passwords. The full interview is available here on the Ashby Village YouTube channel.

Recommended Password Features

There are three recommended features to a secure password.

- *Complex*: A strong password generally contains a combination of CAPS, small letters, numbers, punctuation. Passwords should be complex, but "complex" does not mean completely arbitrary. The password can be readable.

- *No personal information*: Do not include: your birthdate, address, phone number, family names, or pet names. Excluding personal information will make it harder for a hacker to guess your password.

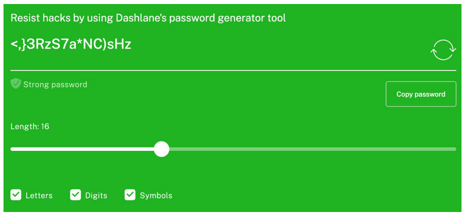
- *Unique*: You should use a different password on every site. And do not use the same password repeatedly over time.

These three features allow you to choose three paths to improving your passwords! Begin working on any one of these to get started:

- creating more complex passwords
- deleting personal information from passwords
- replacing repeated passwords with unique passwords

Online resources can help you.

For example, click Secure Password Generator for a tool that helps you construct a password to the specifications required on a particular website - length, letters, digits, symbols.



Resist hacks by using Dashlane's password generator tool

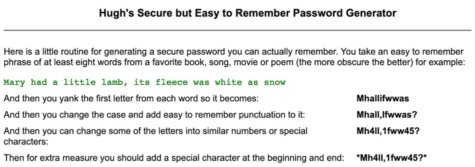
<,}3RzS7a*NC)sHz

Strong password

Length: 16

☑ Letters ☑ Digits ☑ Symbols

Hugh's Password Generator offers a fun way to generate a password from a favorite book, song, movie or poem.



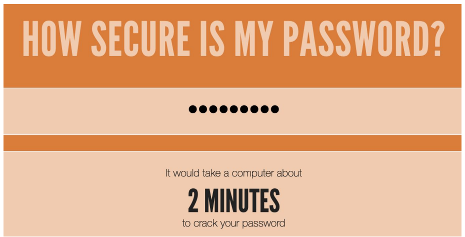
Hugh's Secure but Easy to Remember Password Generator

Here is a little routine for generating a secure password you can actually remember. You take an easy to remember phrase of at least eight words from a favorite book, song, movie or poem (the more obscure the better) for example:

`Mary had a little lamb, its fleece was white as snow`

And then you yank the first letter from each word so it becomes:	**Mhallifwwas**
And then you change the case and add easy to remember punctuation to it:	**Mhall,lfwwas?**
And then you can change some of the letters into similar numbers or special characters:	**Mh4ll,1fww45?**
Then for extra measure you should add a special character at the beginning and end:	***Mh4ll,1fww45?***

And this tool, How Secure is My Password, estimates the time it would take a hacker to guess your password. In the example at right, we typed "mydogfido," and that password is guessable in just 2 minutes!



It would take a computer about

2 MINUTES

to crack your password

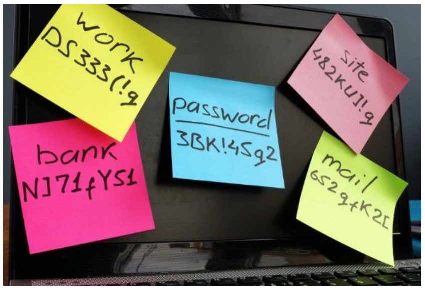
Password Records & Storage

Remembering and organizing passwords can be very challenging. You may have a complex password, and it may be unique, but it's of no use if you can't find it!

In this section, we describe four methods of recording and storing passwords:

1. Sticky notes
2. Written list
3. Browser storage
4. Password manager

1. Sticky notes

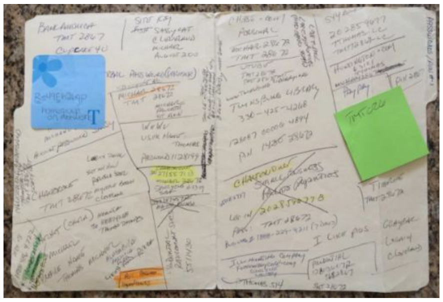


We’ve all used this method - jotted a password on a sticky note and stuck it to our computer. The advantage is that sticky notes provide an easily accessible record! But let’s admit there are disadvantages. Sticky notes may be difficult to read, are hard to organize, can’t be easily stored in a secure location, and can’t be easily shared with family/friends.

2. Written lists

Written lists are an advance over separate sticky notes. There are three common approaches to lists:

- Handwritten list
- Handwritten logbook
- Typed



A handwritten list like the list in the photo is an easily accessible record, can be stored in a secure location, and can be shared. But it may be difficult to read, and it is difficult to reorganize.

A handwritten logbook is a more advanced list option for alphabetizing logins and passwords. A logbook organizes your website logins alphabetically, is easily accessible, can be stored in a secure location, and can be shared. The example in the photo includes lines for site name, web address, username, and password. There are many advantages to a logbook, but, if you want to share your passwords, copying requires duplicating it page by page.

A typed list is an alternative to handwritten lists. A typed list can be easily read, alphabetized, stored, and shared. If you decide to type up your passwords, be sure to include website name, website URL, login/username, and password. We also recommend including the date you created the password to keep track of password changes. You can store your typed list on your device (but please name your file something other than "my passwords"!), or you can print it for storage. Store a copy "in the cloud" for use when you're away from home.

3. Browser storage

A third method is storage in a browser - like Chrome, Firefox, or Safari - or storage in your smart device - your smartphone or tablet. Browsers and devices build in their own password managers.

Each browser and device handles password storage a bit differently, and space does not permit us to describe them all. But most include the options to:

- keep all saved passwords secure with a master password
- save passwords selectively
- generate a complex password when you create or revise a password
- sync passwords across your devices

There are advantages to browser and device storage. Storage is convenient - you just log in with a master password; there's no need to alphabetize; the app can generate a complex password for you; and there are security features built in. But there are disadvantages. Each browser or device stores passwords separately; browsers and devices must be updated regularly to ensure the latest security features; you will be most secure if you log out of sites after visiting them; you must remember your master password; your passwords can't be easily shared.

4. Password manager

A third party password manager is similar to browser storage: You use one master password to store and access all your passwords. The difference is that your passwords are available in any browser on any device! Examples of well-reviewed third party managers include Avast, Dashlane, Keepass, LastPass, and 1Password. Several of these offer free versions.

To get started, you create your Master Password, and then you begin to build the repository or "vault" for your passwords. There are two routes to adding passwords to your vault - moving passwords from your password list or from your browser password storage.

If you have a password list, you'll have to type in your passwords, but you don't have to add all your passwords at once. You can add passwords one site at a time whenever you need to log in. If you've stored your passwords in a browser, there are methods to export those passwords and then import them into your third party manager vault.

While there is some work to setting up a password manager, you can build your vault over time. And one of the many upsides is that converting to a password manager can be an opportunity to strengthen your passwords, one at a time!

We'll use LastPass as an example of a third party password manager. Lastpass offers a number of features typical of most managers:

- requires a master password
- holds your passwords in a "vault" that encrypts your passwords
- offers the option to generate a strong passwords per the requirements on a particular site
- stores secure notes, bank cards, and addresses
- offers both a free version and paid subscription versions
- is available for all devices
- provides tech support

The optional subscriptions cost $36 for Premium and $48 for Family. Benefits of subscriptions include:

- emergency access
- high priority tech support
- multi-factor authentication
- 1 GB file storage

While there are many advantages of password managers, there are some disadvantages as we summarize below.

Advantages	Disadvantages
● works with major browsers and devices ● encrypts your vault, so your vault is highly secure ● generates complex passwords ● stores secure notes ● stores form entries, including address and credit card numbers ● is shareable if you share your login ID and master password with family	● requires memorization of master password ● requires paid subscription for advance features ● may be challenging to learn

If you're ready to install a password manager, we suggest choosing one that's familiar to a friend or family member, so you can ask for their help.

The best password manager is the one
used by someone you trust!

If you're an Ashby Village member, and you're interested in learning more about any of the suggestions in this article, request a technology volunteer by emailing info@ashbyvillage.org or calling (510) 204-9200.