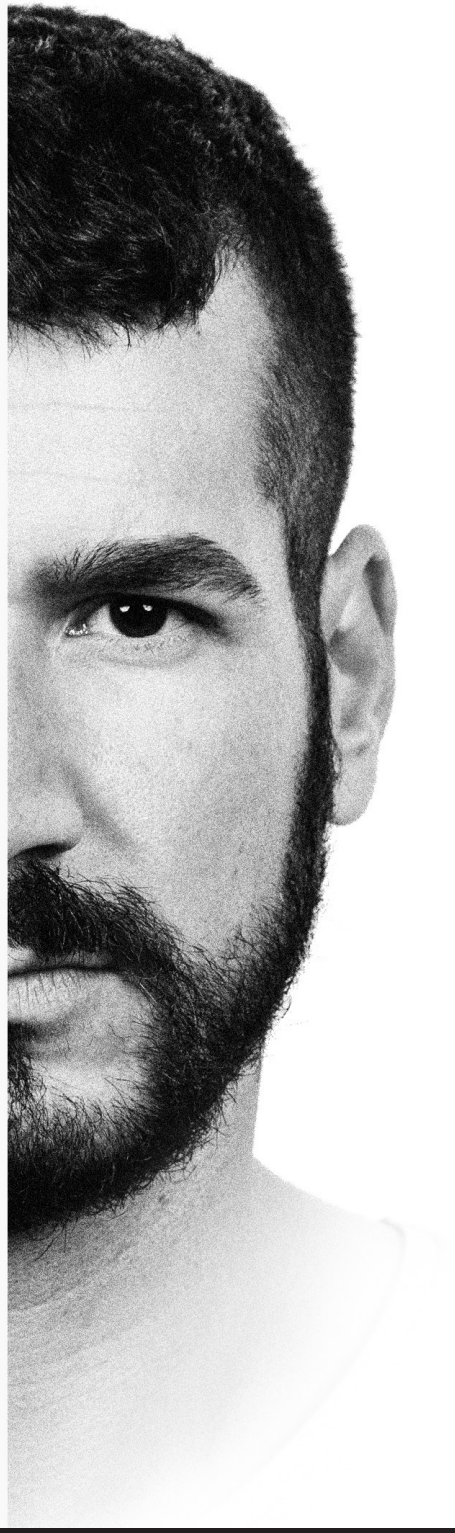
PASSWORD AND PASSWORD SECURITY



A SPECIAL REPORT BY CRAIG PETERSØN

******

Top Tips and Best Practices for Creating and Managing Passwords

WWW.CRAIGPETERSØN.COM

This topic always gets me hot under the collar. Let me share a story with you.

I have a daughter who is a mariner. That means that she sails in shifts of 3 months on three months off. Yes, on the open ocean and away from shore and therefore internet access. She was also a Navy Officer during this part of her career. The Navy had a policy that she had to change her password every 90 days - not necessarily unreasonable.

However, it meant that she would have to log in and change her password or it would lock her out of the network while she was at sea. Of course that means that she was always getting locked out of the Navy system, which the Navy required she use. The Navy also had designed a complex system that must be followed and you had to know (remember) your old complex password to change it. However, there was no flexibility in the process to take into account that she was AT SEA without INTERNET ACCESS for three to six months at a time. It made all her contact with the Navy training network near to impossible.

It continued for the entire time she was in the Navy. In fact, the password requirements the Navy had was the main reason that she resigned her commission. If they had allowed some flexibility in password generation, say longer but less complicated word strings, she might have been able to remember her password even when she did not use it regularly. That combined with a longer time-to-expire, or the ability for her to use her old password to generate a new password once when she finally got online, she would probably still be a Navy Reserve Officer.

As a businesses, we need to consider when and how our employees need access to our networks and have some flexibility for employees who travel. If there is a hard and fast password change policy and an employee is traveling, they may find themselves locked out during an important negotiation or emergency.

Well now let's get down to "brass tacks" of Passwords

Many businesses insist that their eight character passwords are secure because they force complexity requirements.

Not true.

Let's look at password length from a mathematical point of view. Using a passphrase always increases security.

Let's look at a worst-case scenario. What if the hacker is someone like Ken Jennings the Jeopardy champ who has a knack for remembering things -- it is possible that by knowing that all the passwords are made up of only words from the dictionary how quickly could he figure out the password?

Ahh, but what if the person creating the password spells it wrong -- intentionally spells it wrong. Guys, this happens much more often than you might expect. And it does make the password more secure.

My position is that length trumps complexity!

Password policies are all about making passwords hard to guess and the hashes hard to crack.

Crackers typically use two approaches:

Guessing
Choosing a dictionary word or one of the most common passwords, like 123456

Brute Force
Consists of trying many passwords or passphrases with the hope that eventually they will guess it correctly. In many cases, they will only have to guess 50% of the possible passwords.

Having a standard password construction guidelines can come back to bite you because "loose lips sink ships" and if anyone in your organization identifies what your construction guidelines are and it can be over.

Which matters more Complexity or Length?

Let's start with the standard eight character password. We'll assume our average user won't use numbers,

> **"My position is that length trumps complexity!"**

capital letters, or special characters.

What this leaves us with are 26^8 possible passwords. Of course, we're ignoring that users will pick recognizable letter patterns (e.g., words). 26^8 = 208,827,064,576 possible combinations.

What if we teach our users about the magic of the shift key and they start using capital letters? That changes the base to 52, but the exponent remains

the password length. Now we have 52^8. Certainly a marked improvement.

That means that we now have 52^8 = 53,459,728,531,456

What happens if we mix in numbers as well, then we are at 62^8

Check out this Math
26^8 = 208 Billion
52^8 = 53 Trillion
62^8 = 218 Trillion

Now, what if you add in some of the "special characters" available yielding 94^8 or Six Quadrillion

Complexity works, but not if you have to write it down.

Let's talk about length!

Using only lower case letters, so a maximum base of 26 and a string length of 12 we end up with 26^12 or 5 Quadrillion

Merely using a 12 character lower case password with entirely no complexity is better than an eight character password use lowercase, uppercase, and numerical characters.

Longer passwords make it infinitely harder for the criminal to break it. I have argued that we should consider a 15 character password.

Why 15 characters you ask? Well, it all comes down to Microsoft, and some poor code they released. Before Windows NT the primary hash used by Microsoft LAN Manager and Microsoft Windows (LM Hash) was broken. The LM Hash did not allow the storage of passwords longer than 14 characters.

Remembering words is much more straightforward so combining words multiple words we know makes it easier to remember.
How about this "airlinefoodughh."
It's not complicated -- but mathematically it is very secure, and it is pretty easy to remember.

Check this out - it is 26^15=1 ,677,259,342,285,725,925,376 possible combinations.

Complexity cannot beat length when it comes to passwords. Longer passwords are much more secure.

> **"Complexity cannot beat length when it comes to passwords."**

Using a 15 character password creates a very secure password.
26^15 = 677,259,342,285,725,925,376 or 677 quintillions which would make a brute force crack impossible even with the use of a supercomputer.

Let's get real, who is going to remember 15 random letters?

Here are some other phrases that are much easier to remember than "Kr849!@h" "airlinefoodughhmystomach" which is 26^24 or "iwanttorideahorse" which is 26^17

Which passwords above will resist a brute force

attack? Yes, they are the ones that are more natural to remember, they are less likely ever to write it down --- **WINNING!**

Yes, some will say that stringing dictionary words together makes them easier to guess, but that is only if the attacker knows that this how you are creating your passwords and what you would base them on.

Because of bad password policies, users are writing down their complicated passwords, and some are still putting them on post-it notes on their screens or in their cubicles. Allowing them the freedom to design a password they can remember means they are less likely to write it down.

Long passwords will never prevent users from compromising themselves in the physical domain but will thwart attackers trying to remotely brute force an account.

And if your hashes get stolen, you can rest easy knowing that "soupsmellslikefish," while easy to remember, is less likely to be recovered by a cracking program.

Password Managers

In this day and age using a password manager is mandatory. It defends against criminals by generating and storing a different password—even one that's long and complicated—for each of your online accounts. And you only have to remember one password to keep all of your passwords safe!

What is a Password Manager?

A password manager is a tool that helps you generate and retrieve complex passwords across all your accounts. They can also store PINs, Credit Card Numbers, CVV codes and answers to all those security questions. Good password managers save the information in an encrypted form or generate them on demand with rotating, time-based passcodes. And all you have to do is to remember a single password.

You will have access to every login and yet know that it is all securely locked down and encrypted.

The most popular Password managers available today are:

1Password (the one I use and recommend)
LastPass
Dashlane
KeePass and KeePassX

The only difference comes down to the features you prefer.

Getting Started

Here is a basic comparision for my most recommended Password Managers.

	1Password	LastPass	DashLane
Cost	**$2.99/mo** $4.99/mo for 1password Families	**FREE** $2.00/mo for more features	**FREE** $3.33/mo for more features
	Uses AES-256 Encryption		Uses AES-256 Encryption
• Downloadable Software or App	✓	✓	✓
• Browser Extension	✓	✓	✓
• Compatability - Mac - Windows - iOS - Android - Chrome - Firefox - Internet Explorer	✓	✓	✓
• After-sales support	✓	✓	✓
• Storage - Offline - Cloud	✓	✓	✓

It is relatively straightforward for most of them.

Dashlane and 1Password require you to download and install software and as well as an extension for your browser.

LastPass: only a browser extension is required.

With Dashlane and 1Password:

You will download and then install their software along with an extension for the browser you are using.

LastPass: only a browser extension is required.

If you want to use these on your Mobile device, then you will need to download an app.

Next, you will set up an account. It will require your email address and will need to come up with a master password— it should be a long, but not overly complicated one. (see the first part of this article)

Then, you'll have to connect your various accounts with the password manager. Then import your browser stored passwords or have the password manager save both your username and your password, for the next time you log in to a site. Alternatively, you can enter all the information manually.

Unfortunately, you will have to change the majority of your old passwords yourself.

To do this:
Log on to each site, and select your account information, then let your password manager generate a new long, unique password for that site. While you are there, change the answers to your security questions (which you can store in your password vault, too.)

It will take time to replace all your weak or reused passwords, especially if you have dozens of accounts. Don't worry, you don't have to do them all at once, but make sure you change them as soon as you can. Start with your high-value accounts first and then get around to the other ones as you can.

Phishing Protection

The password managers also store the URLs for sign-ins. Why? It's a useful security feature. Hackers use phishing techniques that direct people to fraudulent websites with slightly different web addresses to trick users into submitting their account information. By using the URL stored in your password manager rather than clicking on links in a suspicious email you can protect yourself from this type of scam. Alternatively, you can type the URL yourself.

So, where do they store all my passwords?

There are two different major types of password manager storage. Local and Cloud-Based. You need to decide which you prefer local, cloud-based storage or a hybrid.

By default, LastPass, 1Password, and Dashlane store your password vault on their servers. What this means is that you quickly sync your data across devices.

An additional benefit is that if your computer crashes, you won't lose your vault.

However, you do have the option of storing them locally.

With Dashlane you can disable the "Sync" feature in Preferences. When you do this, you delete your vault and its contents from the company's servers.

However, that means that any further changes you make to your "vault" on your computer will not show up on your other devices.

With 1Password you have another option:
They have a software license purchase for 1Password for a one-time fee of $64.99, which allows you to store your vault where you wish with complete control over it.

The only entirely local password manager is KeePass. KeePass creates an encrypted vault on your local hard drive.

They have procedures for transferring your KeePass password file for use on your mobile device.

For instance, the iOS app MiniKeePass can send the "vault" to your iPhone via iTunes.

Password Sharing

You should always strive to keep your passwords private. However, there are situations in which you might need to share a password with one or more family members or a co-worker.

I use 1Password because it has both a business and a family subscription option that allows five family members. The cost is only $4.99 per month.

It enables us to share access to programs to which family members need access.

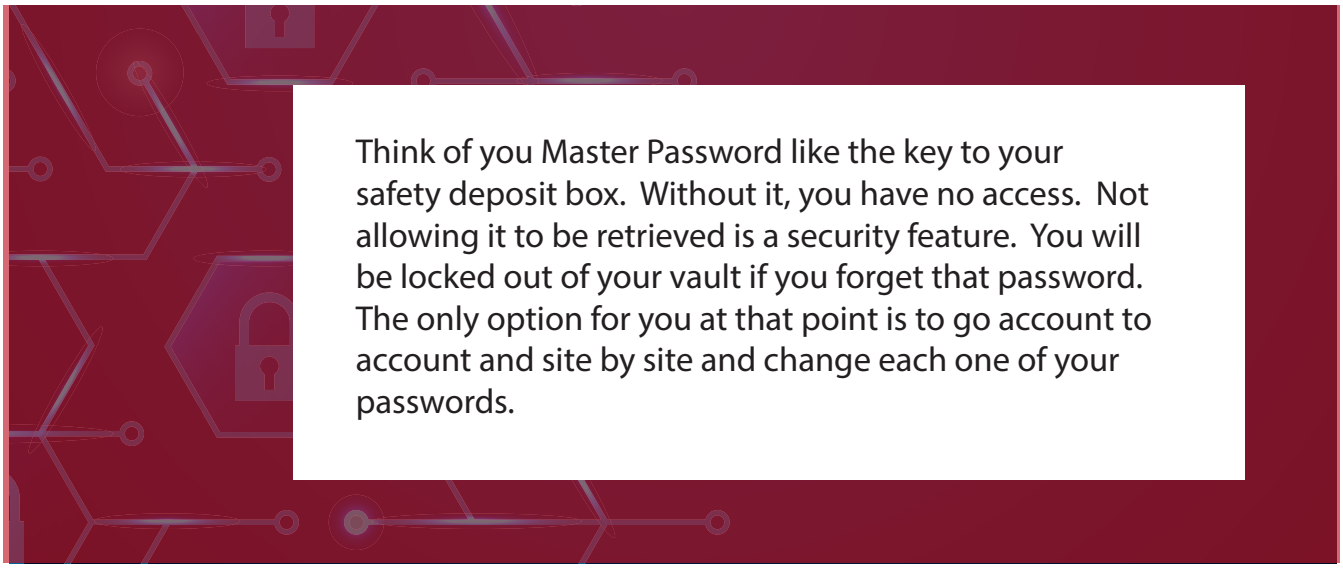
Each member will need to download 1Password and create their master password then they will have access to the family vault. Any changes made to the family vault will sync to everyone's device which has access to that vault.

The paid version of LastPass allows you to share passwords with unregistered users. However, if they want to get those passwords, they have to sign up for a free account.

The paid version of Dashlane also allows you to share passwords with unregistered users. However, if they want to get those passwords, they have to sign up for a free account.

Although there are free versions of these applications, they come with restrictions.

Don't Forget Your Master Password



Think of you Master Password like the key to your safety deposit box. Without it, you have no access. Not allowing it to be retrieved is a security feature. You will be locked out of your vault if you forget that password. The only option for you at that point is to go account to account and site by site and change each one of your passwords.

To read more about Password Security articles visit:
https://craigpeterson.com/?s=password

I'm always looking for your feedback. To let us know what else you think we should add to this Special Report, or to give us some suggestions for other Special Reports, go to **https://craigpeterson.com/contact-me/**