**Passwords to Passphrases**

To create a secure password we should first consider how most of them are broken:

• Overuse

• Easy Access

• Brute Force

I’m sure we are all guilty of using the same password for multiple access requests, often because we find it difficult to remember many passwords & their uses. This then leads to the next problem, where do we store them. The Post-It note on your computer monitor is not ideal, nor is the easily opened ‘locked’ Excel spreadsheet.

When it comes to ‘hacking’ a password, many of us envisage a hooded youth tapping away at his keyboard, attempting to guess the combination. The reality is more automated & much more powerful. The ‘brute force’ method sources a global library of data, including information about yourself & your lifestyle, in sync with multiple computers. Then they simply try every combination they can think of…! The trick with password security is to slow them down.

Rules to creating a secure password have changed over time, & with the introduction of biometric security, it may be only a matter of time before they are no longer needed. A successful password needs to be both memorable & secure. If you follow up with secure password storage, you may only need ONE master password.

**The easiest way to increase password security is to make it longer - 12+ characters**

This leads us to the transition from Password to Passphrase, to assist the recall of a long combination. A passphrase is a string of memorable words, with the possible addition of a few choice symbols & numbers, but they are not without their own security risks. For a passphrase to be secure the chosen words must be the opposite of the famous psychiatric word association tests, there must be no entropy, no connection between them.

Some bad examples showing entropy are:

ChalkCheeseWine  
WilliamHastings1066  
JohnPaulGeorgeRingo

The more words, the more secure the passphrase becomes, it doesn’t matter if the words are short & they don’t have to be nouns.

**For a Master Passphrase, you should aim for 4-5 words.**

Some examples:

CocoaBallKeyBlowJumping  
TravelPantherSixOffDrive  
SmartBagHappy12Dark  
Things\*HomeCardPie

The individual words do not need capitalising …I just did this for clarity in the example. For less secure requirements, 3-4 words should do.

For words sources, you can look around you & pick up random suggestions from books, letters, webpages, sounds, smells …use all your senses! Once you have compiled a candidate, look at it again & search for patterns. Check for subject matter & journalistic styles, especially if you used a single source , such as your favourite cookbook. If you see a word that may have a connection …simply replace it, until you are satisfied.

You now have the **Master Passphrase** & can progress to storing & securing your precious treasures…

=========================================

**MarkDown**…

![password-header][1]

\*01st January 2022\*

To create a secure password we should first consider how most of them are broken:

\*\*- Overuse

- Easy Access

- Brute Force\*\*

I’m sure we are all guilty of using the same password for multiple access requests, often because we find it difficult to remember many passwords & their uses. This then leads to the next problem, where do we store them. The Post-It note on your computer monitor is not ideal, nor is the easily opened ‘locked’ Excel spreadsheet.

When it comes to ‘hacking’ a password, many of us envisage a hooded youth tapping away at his keyboard, attempting to guess the combination. The reality is more automated & much more powerful. The ‘brute force’ method sources a global library of data, including information about yourself & your lifestyle, in sync with multiple computers. Then they simply try every combination they can think of...! The trick with password security is to slow them down.

Rules to creating a secure password have changed over time, & with the introduction of biometric security, it may be only a matter of time before they are no longer needed. A successful password needs to be both memorable & secure. If you follow up with secure password storage, you may only need ONE master password.

\*\*The easiest way to increase password security is to make it longer - 12+ characters\*\*

This leads us to the transition from Password to Passphrase, to assist the recall of a long combination. A passphrase is a string of memorable words, with the possible addition of a few choice symbols & numbers, but they are not without their own security risks. For a passphrase to be secure the chosen words must be the opposite of the famous psychiatric word association tests, there must be no entropy, no connection between them.

Some bad examples showing entropy are:

- ChalkCheeseWine

- WilliamHastings1066

- JohnPaulGeorgeRingo

The more words, the more secure the passphrase becomes, it doesn’t matter if the words are short & they don’t have to be nouns.

\*\*For a Master Passphrase, you should aim for 4-5 words.\*\*

Some examples:

- CocoaBallKeyBlowJumping

- TravelPantherSixOffDrive

- SmartBagHappy12Dark

- Things\*HomeCardPie

The individual words do not need capitalising …I just did this for clarity in the example. In some cases, I substituted a symbol or number for a word. For less secure requirements, 3-4 words should do.

For words sources, you can look around you & pick up random suggestions from books, letters, webpages, sounds, smells …use all your senses! Once you have compiled a candidate, look at it again & search for patterns. Check for subject matter & journalistic styles, especially if you used a single source, such as your favourite cookbook. If you see a word that may have a connection …simply replace it, until you are satisfied.

You now have the \*\*Master Passphrase\*\* & can progress to storing & securing your precious treasures…

[1]: http://johnwalton.photography/words/content/images/20220101164133-20220101\_john-walton\_password\_001e-1.jpg