HOW TO CHOOSE A SECURE AND MEMORABLE PASSWORD FOR YOUR 'PASSWORD PROTECTED PDF FILE'

*****Go to www.bitgoldwallet.com for information on what bitcoin is and how to safely buy, use and store it, and how to choose a secure and memorable password*****

TRIPLE 7 / 11 / 7 PASSWORD
(STEP BY STEP NOTES)

1. Choose a password that is exactly 32 characters long. PDF formats version PDF1.6 and older have a password character limit of 32 characters, so choosing a password of greater character length would be complicated to use.

2. Choose your password from all the letters of the alphabet (upper and lower case) and the numbers 0-9. The password must contain both capital and lowercase letters but it doesn't have to include numbers. Don't include punctuation marks or spaces or any other character types.

3. Choose this password by coming up with 4 sentences. Each of the first three sentences must have at least 7 words in them and the 4th sentence must have at least 18 words in it. The 4th sentence can be made up of 2 or more sentences as long as they are connected sentences. We will be taking the first letter or number of each word in these sentences to create your password.

4. The first three sentences must be from three different sources either from a **b**ook, **c**omic book, **d**ocumentary, **m**agazine, **m**ovie, **s**ong, **t**elevision program episode, or **v**ideo game, available online that has been widely published (widely = google/youtube etc. can find it). Although widely published, the less popular the source item is, the better. The sentence can't be a common phrase like 'the quick brown fox jumps over the lazy dog' but must be memorable and must be from a favourite thing of yours (ideally from your childhood or teenage years, but not necessarily). On top of this, no one besides you can know that these are your favourites and there can be no copy of this favourite item on any online email account/website/online blog or internet connected computer of yours. This includes not already being used as a security question answer of an online website account of yours. If a security question answer has already been used from a source you want to use (eg. book), you can choose your second favourite thing from that source (ie. second favourite book).

5. Each sentence of the first 3 sentences must come from a different source (eg. favourite book and favourite TV program not both from favourite books). When researching these 3 sources only do so either from a public computer or from your personal computer using a secure Linux usb operating system that you are sure has no spyware on it.

6. Examples of different good 'widely published' favourite sentences are the 1st lyrics of the song "Graduation" by Vitamin C, and the memorable quote from the movie Rocky 6 "Let me tell you something you already know". Basically, whenever you think of the movie or book or source, you will be able to easily remember or find the sentence. Choose a sentence which you can actually go to, to read or listen to again. And the source should be something that will be around forever. Also, to make it easier to remember the order, arrange the 3 sentences in alphabetical order of the source (eg. book first since it begins with the letter b).

7. The fourth sentence needs to be the exact opposite of widely published (opposite = cannot be found online). It must be unique and memorable, and must not be from a source or part of a source that is published online anywhere. It must also not be stored on your internet connected personal computer. It can only come from something you or someone else you know, has said or written that is in a video, voice recording or written article stored in your home (and only your home, not someone else's), which you have access to and will continue to have access to indefinitely into the

future. The 4th sentence can be two or three different sentences provided they are consecutive connected sentences from the same part of the source.

8. Examples of different 'opposite-of-widely published completely offline' sentences are something you or someone else said in a family video of yours, or a sentence from a cherished old school essay you wrote, or a private personal letter given only to you (or by you) to someone close to you which you have at home on a digital storage device or physical file. Or, it could be from any other memorable written article or voice recording or video recording you have made but not published online.

9. The reason why we want these sources to have originally been from something in writing, or in a voice or video recording somewhere, is so there is a backup incase you forget the exact wording of the sentences. It is way easier to remember the source articles than it is to remember a phrase alone. For most of the sentences, the first sentence from the source article should be used so it is easy to remember where the sentence came from, however for at least one of the first 3 widely published sentences another memorable location other than the first sentence must be used. Remember though, that it must be memorable to you (for example; after a major part of the book or a popular quote in the movie).

10. The reason why we want these sources to be your personal favourite items (particularly from your childhood or youth) is so that you will be much more likely to remember them. They will be unique to you and will be words you will always be able to work out, even into old age. The reason we want at least one of the first 3 sentences to be from a memorable location as opposed to the first sentence only is so that it will dramatically increase the overall brute force difficulty of your password (since a computer often won't be able to distinguish between a memorable and unmemorable part of the source and will hence need to try every possible 7 word sentence portion from that source).

11. Now for the first **"7 / 11"** portion of the password: take the first letter or number of each of the first 7 words of the first 3 sentences and use these as your password. Then take the first 11 letters or numbers of each of the first 11 of the 18 words of the fourth sentence (or connected sentences) and add this to your password. Correct capitalization is needed so if the word starts with a capital letter, use the capital letter.

12. Now for the final **"/ 7"** portion of the password: Take the first letters of the last 7 of the 18 words of the fourth sentence (or connected sentences) and replace the 2nd, 3rd, 9th, 10th, 16th, 17th and 23rd characters of your current password in the right order. These are basically the 2 characters immediately after the first letter or number of each of the first 3 parts of the password; and the 1 character immediately after the first letter or number of the 4th part of the password. Correct capitalization is needed so if the word starts with a capital letter, use a capital letter. This part is important but is a little tricky to understand. It is however clearly illustrated in the example password given here:

EXAMPLE PASSWORD:

1st sentence = "Rocky 6" memorable quote = **L**et **m**e **t**ell **y**ou **s**omething **y**ou **a**lready know.
2nd sentence = First lyrics of "Graduation" song by Vitamin C = **S**o **w**e **t**alked **a**ll **n**ight **a**bout **t**he rest of our lives.
3rd sentence = The "Simpson's 'Radio Bart' episode" main song = **W**e're **s**ending **o**ur **l**ove **d**own **t**he **w**ell.
4th sentence = First two sentences of old school essay = **S**alaries **o**f **m**illions **o**f **d**ollars **a** **y**ear **a**re **p**aid **t**o **i**nternational **e**ntertainers. **I**t **c**an **b**e **a**rgued **t**hat **s**uch large amounts are not warranted.

Final password =

- First 7 characters of 1st, 2nd and 3rd sentences (keeping capitalization where it exists) [First 3 sentences are arranged in alphabetical order of source: first sentence is a movie (m), second sentence is a song (s), third sentence is tv show (t)]. +
- First 11 characters of 4th sentence (keeping capitalization where it exists) +
- Last 7 characters of the 4th sentence replacing password characters in places 2, 3, 9, 10, 16, 17 and 23 of the password (keeping capitalization where it exists and using correct order).

Final password =

Triple 7 / 11 portion of password = **LmtysyaSwtanatWsoldtwSomodayapti**
Last 7 portion of password = **eIcbats**
Final Triple 7 / 11 / 7 password = **LeIysyaScbanatWatldtwSsmodayapti**

LeIysyaScbanatWatldtwSsmodayapti

13. **And that is it...** you have your new super secure, easy to remember password.

    To help you remember the password; on at least one securely backed-up copy of the password protected encrypted PDF file you must include in the file name, the hint to the password such as the words '32 character Triple 7-11-7 password, movie, song, tv program + personal phrase hint (not the source name)'. It is however strongly recommended to include the password hint in the name of ALL copies of the PDF file, so there is a much lower risk you will not be able to remember your password.

Note: Remember the length rules by remembering the phrase **'Triple 7 / 11 / 7'**.

DISCLAIMER

This entire password procedure is a work in progress only. It hasn't been thoroughly tested and comes with no guarantees of any kind whatsoever. Only use it at your own risk. Furthermore, these notes are offered here purely for information purposes, and anyone affiliated with this work accepts no liability whatsoever for any circumstance that may arise out of the information provided.

CHECKLIST

PASSWORD MUST

- Be 32 characters long
- Contain both capital and lowercase letters (and optionally numbers)
- Have the first 21 characters of the password be made up of the first 7 letters (or numbers) of 3 different widely published sentences available online, maintaining correct capitalization.
- Have the 3 online available sentences used to make the password come from either a **b**ook, **c**omic book, **d**ocumentary, **m**agazine, **m**ovie, **s**ong, **t**elevision program episode, or **v**ideo game.
- Have the 3 online available sentences used to make the password be from a favourite thing of yours, which no ones else knows is your favourite thing, and which isn't in any online email

account/website/online blog internet connected computer of yours or used as a security question answer of an online website account of yours.

- Have the 3 online available sentences used to make the password be sentences you can actually go to, to read or listen to again, indefinitely into the future.
- Have the 3 online available sentences used to make the password be arranged in alphabetical order according to the source (for example: book first since book begins with the letter b).
- Have the 3 online available sentences be from the first part of the source or from a memorable part of the source (source means book, comic, movie etc), so it is easier to remember. It must be from a memorable part of the source and not the first part of the source for at least 1 of the 3 online available sentences.
- Have the last 11 characters of the password be made up of the first 11 letters (or numbers) of a unique 18 word part of a sentence or connected sentences, that is from a memorable part of a source, available only in your home. The sentence must not have been published online and can be something such as a family video, or cherished old school essay, or private personal letter, or other private written article, voice or video recording. The source must always be available for you to access again indefinitely into the future. Correct capitalization needs to be used.
- Have the 2^{nd}, 3^{rd}, 9^{th}, 10^{th}, 16^{th}, 17^{th} and 23^{rd} characters of the current password after the above steps have been completed, be replaced with the first characters of the last 7 letters (or numbers) of the unique 18 word part of a sentence or connected sentences mentioned above. Correct capitalization needs to be used.
- Must have a password hint included as part of the name of at least one securely backed-up copy of the file that is being password protected (however it is strongly recommended to have it on all copies of the file). This means the file name should include something like '32 character Triple 7-11-7 password, movie, song, tv program + personal phrase hint' to help you remember the password.

PASSWORD MUST NOT

- Have punctuation marks or spaces or characters other than capital upper and lowercase letters and numbers.
- Be made from any sentences that are common phrases like "the quick brown fox jumps over the lazy dog".
- Continue to be used if your home is raided by the government or police. It needs to be changed in this situation.

WHY WE BELIEVE THIS PASSWORD IS UNCRAKABLE

The first three parts of the password (the three public sentences) are designed to be difficult to brute force if properly chosen, and impossible to brute force if cleverly chosen. The number of minimum possible combinations is large even with intelligent guessing methods (conservatively estimated to be at least 10,000 x 10,000 x 10,000 possible combinations = 1×10^{12}; and reasonably estimated to be at least 1,000,000 x 1,000,000 x 1,000,000 = 1×10^{18}). Nation state spy agencies and other large setups may be the only kind of organisations with the capacity to brute force these within a reasonable period of time and only if the opportunity is there. The maximum possible number of combinations for this part of the password is about 62 to the power of 15 which is roughly 7×10^{26} if perfect sentences have been chosen. This is a very large number however, in the event that the sentences are not obscure enough sentences there is an opportunity for this portion of the password to be discovered, if used by itself.

Which leads us to the last part of the password: the private sentence or connected sentences. This sentence (or connected sentences) is designed to be practically impossible to guess on its own without actual access to the source files, but to be definitely IMPOSSIBLE to guess when added to the first part. To brute force this second part alone without knowing the source files will add at least another minimum 1×10^{23} possible

combinations with intelligent character frequency guessing (search “english letter frequency” online). This is a conservative estimate formed by taking 23 to the power of 17. A maximum estimate would be 62 to the power of 17 which is roughly 2×10^{30}. Since a powerful adversary trying to steal your password is unlikely to ever be able to physically enter your home to obtain all the possible hard copies of the source articles that may have been used to create the last 18 characters of the password; we can assume that the last 18 characters used to create your password will always make the password at least 1×10^{23} times more difficult to brute force (which essentially means impossible to brute force when used with first 21 characters).

So multiply the minimum strength of the first part 1×10^{12}, with the minimum strength of the second part 1×10^{23}, and you have 1×10^{34}. That is close enough to the number of possible combinations in an AES128 encryption key (approx. 3×10^{38}) to make it very secure.

Your password is very secure… provided the government doesn’t raid your house.

If a government organization does storm your house one day and confiscates all your things with the intention to try to discover your password, then in that situation you have to look at your password as being compromised and in this situation, you should change your password as soon as it is safe to do so or otherwise transfer all your bitcoins stored using this password into newly created public addresses secured with a new password.

*****Go to www.bitgoldwallet.com for information on what bitcoin is and how to safely buy, use and store it, and how to choose a secure and memorable password*****