Additional notes on The deal about passwords

The related blog post The deal about passwords helps explain the question “What are NIST and all the radio people saying about acceptable passwords?” In this article we go into some specifics about why a good password is good and give you some resources to select an appropriate password.

Arguments against long passwords

Long passwords are typically described as a phrase or sentence that is familiar to you. It could be a line from a poem, the opening line of a book, or anything you are able to remember easily.

- Are they really memorable?
  At the right is a sentence you may have learned in typing class. But look closely. Did you type them all exactly the same? Even if you know what it says, your fingers may not cooperate.

Now is the time for all good men to come to the aid of their country.
Now is the time for all good men to come to the aid of their party.
Now is the time for all citizens to come to the aid of their country.
Now is the time for all good men to come to the aid of their country
now is the time for all good men to come to the aid of their country.

- *And*, are they unique?
  The situation gets more complex if you’re trying to come up with a phrase for more than a handful of sites.

- Are they really easier to enter?
  If you’re not a touch typist, 15 words will probably take you longer to enter than 15 random characters; especially if you can’t see the result of your keystrokes. And, whether you type or not, the effort is multiplied if you have to enter it on a small touchscreen.

- Can you use it?
  Amazingly, even now, some high value sites and many smaller enterprises do not allow free-form, indeterminate-content passwords. They may restrict you to a finite character set or a narrow band of character count. Even without explicit, obvious constraints, they may truncate the length or convert text to all caps (or all lower case) before validating you.

Unfortunately, the fault here is often the use of archaic operating environments or software. At one time, UNIX-based systems only used passwords that were lower case alpha and between 4-8 characters.

Such a password, well randomized, could take up to seven years to brute-force crack. But, if it were “password”, “qwertyui”, or any other word in your *Webster’s Collegiate*; the hacker would be in in seconds.

Creating a good password

These tips are strictly mine and, while they are an amalgam of information from multiple reliable sources, they have not been vetted by anyone else. Take them as a starting point to developing a technique that works for you and avoids many of the issues we've raised.

- ### Determine the quality of the password

  Some sites require you to log in but don't have any personal data or risk if your account were compromised. Others such as financial, shopping, or medical sites have data that could be expensive or inconvenient if lost. The latter should be protected by the best password available.

  A trivial password may be appropriate for non-critical sites. It may be a phone number you remember such as that of a childhood friend. It could also be a string of words with padding to extend their length. Even if it's not valuable, the password should not be associated with you now to avoid leaking current personal data.

  A strong password should be completely random and ideally 12 to 20 characters or more. To ensure the quality of the content you should use a password generator.

- ### Use a password generator

  Most people when asked to create a random password tend to fall into patterns, whether consciously or unintentionally. Most password managers have a tool to create truly random passwords or you can use a stand-alone generator or website. They usually allow you some control over factors such as length, character set, and complexity.

  Here are some other sources for generating passwords:

  - https://www.programming.de/download/archive/password.zip
  - https://www.grc.com/passwords.htm
  - https://map.what3words.com/
    This site has assigned a 3-word combination to *every* 3 meter square parcel of the globe. You can generate a password by selecting a memorable spot that you can hint with a reminder such as "Mom's front door" or "first kiss." The site separates the words with a period. Be sure you use a different character instead.

- ### Use a password manager

  The first rule is to use a unique password for every site. This means you will have dozens to hundreds of passwords to associate with their usage. And, since you're looking up the password and pasting it into a box, there's no excuse not to use a high-quality password for each site. Most password managers can also securely store other data so it's useful not just for web logons, but other programs or credit card emergency numbers.

  If you choose a free, or worse, ad-supported manager; they may be paying their expenses with your data.

  You can't go wrong with the top three, highly rated password managers:

  - Keepass:
    http://keepass.info/
  - LastPass:
    http://s.zaitech.com/SignupForLastPass
  - 1Password
    https://1password.com/

  Keepass is free and open source.
  LastPass and 1Password have free and paid versions.

  You can also use the old standby of a notebook or spreadsheet. You just need to be certain that they will never be lost or accessible by anyone not authorized. If you keep a file in an online account, then it must be protected by a unique password itself.

  Allowing your browser to save passwords is not recommended. They are not assured to be secure and all your passwords could be lost in a system failure.

There's more to come.

This article may be incomplete at this point. Please check back in a couple weeks for even more details.

https://fromthehelpdesk.blogspot.com/2017/08/the-deal-about-passwords.html
http://TechnologyInterpreter.info
https://zaitech.com/satellite/contacts.htm