Strong Passwords

WHY do we need strong passwords?

Because when we use online accounts to carry out transactions for buying, selling, banking etc, we need to make sure that these accounts cannot be accessed by anybody else.

Examples of poor passwords:

123456, password, 12345678, qwerty, abc123, 123456789, 111111, 1234567, liverpool123.

Strong Passwords

Strong, secure passwords are essential on a computer.

Here are two examples, each with 12 characters:

<M{*L2%w24KT h2<{49%M4+YR

The reason that so many people choose weak passwords is because the term "pass***WORD***" is totally misleading.

The very last thing a password should be is a recognisable **word**.

A strong password should:
- Not resemble any of your previous passwords.
- Not be your name, your house name, your telephone number, your friend's name, your pet's name or family member's name or anything related to you that is easily guessable.
- As mentioned earlier, it must **not** be a dictionary word, common name or place name.

The chosen password length is often ***too short***. Also, roughly 40% of all passwords only use ***lowercase*** letters. These are far more susceptible to being broken by "brute force" cryptanalytic attacks.

http://en.wikipedia.org/wiki/Brute-force_attack

How to create a strong password

Rule 1 – Password **Length**: Longer is stronger. Create long passwords at least **12** characters in length.

Rule 2 – Password Complexity: **Complex** will perplex. At least one character should come from each of the following 4 groups.

The more special characters, from the fourth group, the better.
1. Lowercase letters (abc…)

2. Uppercase letters (ABC…)

3. Numbers (123…)

4. Special Characters $ % * &) ? ! < @ ^ ; (~ ” , : - _ = + >

Over a period of time you will accumulate a large number of different passwords and usernames.

Contrary to the advice of some people, you **do need to write down** these passwords and then keep them very safe, well-hidden and secure.
No less a person than security expert Bruce Schneier recommends this:
https://www.schneier.com/blog/archives/2005/06/write_down_your.html

The alternative is to use a password manager.

NB Never use the **same password** for everything, because if one account is hacked, they are all hacked!

If your current passwords are weak, then **change them**!

Please note that some online companies and other organisations do not allow the use of certain symbols or special characters in their passwords. Try them first and see.

Creating strong passwords

******Create and write down*** your new password **BEFORE** entering it online, so that you have a record of it!

REMEMBER: Longer is ***very much stronger*** and ***complex*** will ***perplex***.

Use a combination of:

Lowercase letters	a b c	(26 options)
Uppercase letters	A B C ……….	(26 options)
Numbers	0 1 2 3 ……….	(10 options)
Symbols	? @ (& % $ “ ! } @ ; : . < …………	(34 options)

26 + 26 + 10 + 34 = 96 choices for each character.

Even a 4 character password such as **h?6K** has 96 x 96 x 96 x 96 combinations.

4 characters: 84,934,656 (85 million) The UK lottery odds are 45 million to 1.

8 characters: 7.2138958e+15 (7.21 000 000 000 000 000) (7,210 million million)

10 characters:
6.6483264e+19 (66.4 000 000 000 000 000 000) (66.4 million million million)

12 characters 6.1270976e+23
612 000 000 000 000 000 000 000 (612,000 million, million, million)

NB Always use at least **12** characters.

Use a ***different*** password for each individual account, **NOT** the same one for all.

Ultimate Guide to strong passwords: (Google for "ultimate guide to strong passwords")
http://www.thegeekstuff.com/2008/06/the-ultimate-guide-for-creating-strong-passwords/

NB The first time you use the new account, you will get this message from Firefox:

Remember password?

Click on the Down arrow, highlight and c/o **Never** for this site.