Passwords - the why and how?

**Why do passwords exist?**

Passwords are often what stands between you and access to your data or systems. Although often seen as an obstacle, they should be considered the key - something to be possessed only by those who have the right of access. Like keys, passwords are something to be looked after carefully, reported when lost or given to the wrong person, changed occasionally or when required (if it gets into the wrong hands) and be of a good quality. You wouldn’t use a key for your car that works on every car of that make - would you? Don’t use a password that anyone can guess.

**Choosing a good password?**

Well, first, what do we mean by good? A good password is often referred to as a strong password which is probably a better term as it is less personal. A strong password is one that is difficult to guess, not easily broken and can be easily remembered - because it stops being strong if you have to write it down somewhere where you can refer to it easily. Note: it is not a complete no-no to write down a password but, if you do, this then needs to be carefully stored - compare with the use of a physical key safe.

**Passwords that are easy to guess**

In this category, you will find passwords that use something that is personal to you - this is often shown on TV - people guess a pet’s name, a spouse’s name or a special date relating to the person whose systems/data they are trying to access. Passwords that are particularly easy to type (e.g. qwertyuiop) are also easy to guess from watching and are in the lists used by the cracking tools (see below). Don’t use anything that is known publicly - that you (or someone else) has put on Facebook, your address (on electoral roll), your Mother’s maiden name (a matter of public record).

**Passwords that are easily broken**

This is the category people don’t often realise is a problem. Someone trying to break into your account will not usually be doing so by manually entering their guesses. They will use freely and easily available “password cracking” tools. These work by going through common passwords (such as Password1! - yes really, this is a common password as it satisfies complexity rules(see later) and is easy for the user to remember), dictionaries (not just English, these attacks can use any number of dictionaries and will likely start with the ones for the country of the target and then the country of the attacker), names (in any language) and passwords set by default by various systems/applications (hence the requirement to ALWAYS change default passwords).
Once you've avoided the obvious, what next? Well, the longer a password is, the longer it takes the tools to crack as it takes them longer to work through all the combinations of letters, numbers and punctuation marks. And yes, the more complex a password, the longer it will take to crack too. However, there is a trade-off between length, complexity and how long you keep the password. If you have a short password (7 characters) which is alphanumeric only, it could be cracked in 4 days. You have to change it sooner - not likely or practical. However, if you have a longer password, say 9 characters which is complex (and of course not something like Password1!), it would take the tools (at today’s speeds) a few years to crack on average. Thus, you would only have to change it if you think someone may have watched you type it in or if your account got hacked into.

A fairly obvious outcome from this is that if you use the same password everywhere and one account or system gets compromised, then that password is useless and you would need to change it everywhere. This may seem overkill, but if hackers break into a system and get the password file, then they often publish this on public websites. So, what you probably want to do is use a set of passwords - less complicated ones for systems that simply require you to register to get at public data (often one-off access) and really good strong ones for your QM account and banks/online shopping (anything that may involve sensitive data or that provides access to other sensitive data).

You may see advice suggesting replacing letters with similar looking numbers. e.g. replacing the letter ‘e’ with the number ‘3’ - since this is such common advice, the cracking tools include the common substitutions, hence this advice is no longer very good.

**Suggestions for choosing/using strong passwords**

- have at least 9 characters
- don't use a name - your name or anyone else’s
- don't use your username/login id
- make it reasonably complex - include upper and lower case alphanumeric and punctuation characters or symbols
- ensure it’s not too easy to watch as you type it - avoid using keyboard patterns
- think of a favourite song/poem and make a password from some adaptation of the initial letters - then you can remember it easily - but don’t go for a very popular song/poem as the cracking tools may well be adapting already (e.g. from Jingle Bells, you could make JbJb;-jatw but obviously do not use this example)
- keep it safely (as you would a bank PIN)
- change your password (wherever you have used it) if you think someone else may have learnt it (including if you think you may have given it away in a phishing attempt)
- change all passwords at least once a year - you may not always be aware of a compromise and hackers do not always use their acquired accounts straight away when they get them.

**...and another thing (or two)**

Be careful when typing your password into a phone/tablet device - these devices usually highlight each character as you type, making it easy to be watched and learnt.

Don’t let systems “remember” you when they offer - it means anyone else using that device can get into a system as you (you will generally be held responsible for any activity carried out using your credentials). Also, it’s a lot easier to remember a password when you use it!