Choosing Good Passwords

Pretty much everyone uses passwords all day every day for one thing or another and yet, most of us are still terrible at choosing secure passwords. This guide will explain how you can create strong passwords that aren't horrible to remember.

Choosing Good Passwords

Avoiding obvious passwords

One of the first things to say is that you should NEVER use anything obvious about yourself (pet's name, your name, your partner's name, your mother's maiden name, your date of birth, phone numbers, favourite colours, etc) this applies to passwords but also remember that if you have easily discoverable information as your password recovery questions then someone may be able to reset your password without actually needing to break into your account at all and social media probably holds a lot of this information about you! In fact, a number of the high profile celebrity hacking cases have been because of poor password recovery question choices which has allowed a hacker to break into the celebrities' personal photos in the cloud.

The old advice for creating a secure password was to have a random string of upper and lower case letters interspersed with numbers and symbols. Something that didn't look anything like a word you would find in a dictionary and that was at least 12 characters long. Something like this:-

UY8&beY!6alPQ:3s

Although that is a 16 character password, there are a couple of problems with it - the biggest of which is that it's incredibly difficult to remember and most people couldn't. This leads to people writing the password down somewhere which is itself a security problem. Password managers provide a possible solution to this (*see the section on password managers later*).

Using randomness for password strength

There are ways to measure how good a password is and one of the best ways is something called "entropy" which is basically a measure of the randomness of the characters in a password.

You really don't need to understand how that works but we can use that as a comparison for how strong some example passwords are. For reference, the 16 character password above has an entropy of just under 78 bits. Thankfully there is now some much better password advice which is to select 4 completely random words that are not related to each other and string them together. For example:-

correcthorsebatterystaple

The individual words have been highlighted so that you can better distinguish them. I don't think anyone would disagree that this password is much easier to remember than the previous example and it is actually more secure as it has over 93 bits of entropy. Even so, that's not the best we can do with this password and a couple of very simple tweaks will make it much better. Those tweaks would simply be to capitalise the first letter of each word and to include a bit of punctuation like this:-

Correct!Horse&BatteryStaple?

This password is now still fairly simple to remember, but has over 140 bits of entropy which is approaching twice as secure as the first password I showed.

Choosing Good Passwords

Password Managers

Another very important aspect of passwords is that you should always try and have different passwords for every single system and service you use. The reason is that there are thousands of instances of websites with terrible security who are hacked. The hackers then steal all of the information they hold which may include your password and even, in some cases, previous passwords you've used with those sites.

Of course, if you have a different password for every site then this isn't a problem because you just change your password for that site and everything is back to normal but most of us can't remember hundreds of different passwords. This is where password managers come into play.

A password manager is a software tool which you typically add to your browser as a plugin. Then you only need to login to the password manager (using a really strong password) and every time you have to login to another website – the password manager will deal with it for you.

As with any tool, there is a bit of a learning curve with password managers but it is definitely worth it and some of them also include security audit functions which will tell you if you've got any issues – such as your password is easily guessable, you are using the same password for multiple sites or even that your user account details have been discovered in leaked data from hacked sites.

The password manager I personally use and recommend to everyone is LastPass.com. There are lots of others but LastPass seem to respond very quickly to security issues and are very open and honest about any issues which is vitally important in this type of tool.

Even if you ignore everything else!

I know this stuff takes effort and getting around to it might be difficult. I can't possibly over state how important it is but even if you don't manage to get around to the rest of the advice in this article then the MOST important piece of advice I can give is – at the very least, make sure you have a completely different and secure password for your email account. The reason is that most websites will allow a password to be reset with an email so if someone can login to your email they can probably login to most of your accounts.

The MOST important piece of advice is to make sure you have a completely different and secure password for your email account.