Technology Corner - Password Management
Broadcast date - 18 July 2023

Hello, I'm Cam Stirling from Technology Connections. Welcome to this Technology Corner discussion regarding Password Management. If you have any topics that you'd like me to cover in future Technology Corner segments, please phone Golden Days Radio on 9572 1466 or you can text us on 0447 096 472.

Passwords and Password Management are almost certainly the topics which cause the most stress for the people whom I help with their technology! How are we supposed to remember all of the passwords that we need for our banking, our email, Mygov, newspaper subscriptions, ABC iView, logins for ticketing services, to name but a few. Every system has different password requirements - some requiring special characters, some with numbers only, some with combinations of upper and lower case letters, some with a minimum of 8 characters. How can we manage our passwords to maximise security, minimise the risk of identity theft and stop ourselves from going crazy in the process?

Amongst the people that I help with their technology, the most common "password management system" consists of a little black notebook with a series of hand-written, multiply crossed-out, non-alphabetically ordered passwords. Whilst very common, one fairly obvious limitation of the little black password book is that if someone were to break into your home, the little black book sitting next to the computer, or in the top drawer, is a reasonably likely target. Another limitation is the risk of loss in the case of fire. How would you access your home insurance policy if a fire destroyed your home and your policy login details?

A more immediate and practical limitation that I see almost weekly with the little black book, is that when we are forced to change passwords, it can be very challenging to keep the book accurately up to date. I have seen countless people frantically looking through the black book, trying to work out which password is current, which one "should have been crossed out" or which one of the multiple entries with the same name (e.g. Ticketmaster) they should try first.

Often this results in multiple guesses which can lead to being locked out, needing to follow the dreaded "Forgotten Password" process, which results in yet another "current password" needing to be updated in the little black book, hopefully on the same page that we will turn to the next time this happens... One partial solution which I have seen help some people is writing the current date next to passwords when they are changed. And not crossing out passwords until the new password has been tested to avoid trying to unscramble a password that has been scribbled over after you realise that you need that password one more time before the new password becomes effective!

I don't suggest throwing your little password book out - it is definitely the most widespread solution in use amongst the people that I help with technology. Here are a couple of tips which might help to simplify your passwords though.

The first tip is what I call "fit for purpose passwords". By this, I mean that there are some systems, like banking, superannuation and Mygov for which I want to have rock-solid, very different passwords to those which I might use for less important systems such as my membership of ABC iView. Many of those little black password books that I have seen over the years include loads of "repeat passwords" which, let's be honest, we have all used over time because we just can't remember 150 unique passwords. I think it's ok to exercise a little bit of "password re-use" for non-critical systems, but I think it's prudent to use unique, very strong passwords for banking and money related systems. "Fit for purpose passwords", I call that.

The next tip is that I think it is ok when it comes to non-critical systems to rely upon password management systems such as Apple Keychains, Google Password Manager, perhaps the password manager in your web browser (Firefox, Safari might offer to "remember" passwords for you) for systems that don't involve money. Choose which systems to allow password management systems to remember your passwords for carefully because you don't want someone breaking into your browser or computer password memory system and then finding the passwords to your banking, your Mygov, your superannuation etc.

I allow Google to manage my iView, my Netflix, my Ticketek passwords, but I make sure that Google does not manage my banking. I also keep a unique, strong password for Google to limit the damage if I accidentally did happen to allow Google to save a password for a critical system..

I have seen a system which I think is probably better than the little black book. I helped a smart lady who had a spreadsheet which she painstakingly maintained with all of the 50 or so systems and passwords that she needed to remember. She didn't write the actual password against the name of each system (e.g. Gmail, bigpond, Westpac, Melbourne Theatre Company etc). Rather, she wrote a small series of codes which she understood. She might write KBD which she understood to mean "Karl's birthday, followed by BP which she knew meant the birthplace of her eldest daughter and so on. In this way, she managed to keep the passwords relatively safe, she had a backup of the spreadsheet stored in Microsoft OneDrive in case her house burned down and rather than "crossing out" old passwords in a little black book, she managed them very carefully in this spreadsheet. I'm confident that security experts could pick holes in this approach as well, but it was the most effective approach that I have seen thus far. I'd love to hear about even better approaches if you're aware of them.

I'm Cam Stirling, from Technology Connections and if you would like any help buying, installing, fixing or upgrading computers, smartphones, iPads or smart TV's, please phone me on 0414 482 542.