Radio Days – 2012-11-17

Tip of the Week – Strong Passwords

During the week I had a client who was worried about losing her passwords. I suggested that she use a program called KeePass. This program allows you to store all your passwords in one password-protected store which is encrypted so that nobody, even someone who has access to your computer, can find out what your passwords are.

There is, of course, a hitch to all this security: KeePass itself is protected by a password and, if you forget this password, you will be locked out of all your other passwords. This means that you must remember the password to your KeePass account: lose it and you lose the password to everything else.

There are, of course, a number of ways of keeping this password safe: you can write it down or, better still, keep it on a USB stick that stays with your keys. However you keep this password safe it is essential that you do so.

One way to make a strong secure password is to start with a line of text. This can perhaps be a line of a poem or a speech that you will remember easily. Then you take the first letter of each word and write that down. The next step is to convert some of the letters to numbers or symbols. This is your password.

As an example: take the first line of the poem *Mary had a little lamb*. This becomes *Mhall* which, in turn, can become *Mh@1l*. This password is far too short (a good password will be at least eight characters, and more is better) so perhaps you had better start with

> Mary had a little lamb,
> Its fleece was white as snow.

This gives you *Mhallifwwas* which can then become *Mh@l1i5w3@s*. This is hard enough to guess if you do not know the starting lines and the algorithm, but perhaps too easy if you do know them. Always pick, as your starting point, something that is not too easy for a stranger who has studied you to guess.

Lost in the Cloud

More and more reports of people losing access to their data when it is stored in the cloud are appearing. This involves all sorts of problems for the people concerned. These problems range from not having access to one of their email accounts to losing access to all of their data. If you are a business person who relies on having access to your data then you are in big trouble.

You can lose access in two ways as far as I can see.

Stolen Email Account

If you use an online email account as your primary account then any person who can guess your password for this email account can use it to get access to all your other accounts like Facebook and Twitter. The way to do this is really quite simple: just change the password to the person's email account so that they cannot use it then use this email account to change the password for all of their other accounts. If you use an online document preparation program then you can also find that your access to your data has been taken away.

This happened to Sarah Palin during the 2008 American election. She lost access to all her accounts because of a lax password (her child's name plus her dog's name) on her Hotmail email account. This account was then used to change the password on every one of her other accounts.

Apart from everything else, you need to make sure that your email password, especially if you have a web-based email account, is not too easy to guess. If you would like a hint for creating strong passwords please read the Tip of the Week above

Your Account Revoked

Another problem which can cause you grief is if the company which holds your data in the cloud decides to revoke your access to your account. A similar thing happened about the time of a royal wedding to a woman whose name was Kate Middleton (not THE Kate Middleton). Someone at Facebook thought that she was using the name of the famous Kate Middleton so decided that her Facebook details should be removed because it was an obvious fake.

Wrong!

This is bad enough, but getting American companies like Facebook or Google to return your emails or calls, let alone your data, is even worse than pulling hens' teeth. They do not want to know that there has been a mistake on their watch so they just ignore you in the hope that you will become bored and stop pestering them.

This is the main reason that I will not keep any of my important data in the cloud.

I might change my mind if the company holding the data is Australian, and hosts your data in Australia, because then you can use the Australian courts or Government departments like Consumer Affairs or the ACCC. With American companies even the bad publicity generated by something going wrong does not give them any reason to reverse their decision to remove access to your data.

Please ensure that you keep copies of your data under your control if you use cloud storage or processing. The first check that you should make before deciding to use any cloud service is *Can I save my own data to my hard disc?*. If the answer is *No* then I strongly recommend that you do not take this cloud option. Data is the most important part of any computer so, if you cannot access your data, then the whole operation is a waste of time.

I am sure that there is a good reason to use cloud operations but I still prefer to control my own data. With some services you lose access to your data if you do not pay your monthly fee. This would be a calamity in my business.

Further Information

KeePass	www.keepass.info