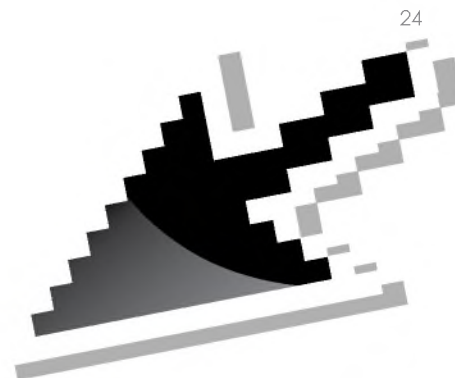


Webb's Web



More on my blog www.alia.org.au/webbsblog

WEBB'S WEB

Let's continue to be real careful out there

It's a good thing that bad things sometimes happen to good people (and here endeth the philosophy lecture). You will probably have heard something of the trials of Mat Honan, a writer for *Wired* magazine, who had various online accounts hacked and as a result lost a lot of personal data. Read his story at tinyurl.com/8q2jwsu. Following the publicity (and the outcry) arising, both Apple and Amazon – whose admittedly lax password recovery procedures had facilitated the hacking – have changed their processes. Now this is going to make life a little more complicated for all of us when we want to recover a password, but I think it's a fair trade off. I've long argued that I don't implement more complicated security on my accounts because of my "risk management" practice, i.e. who's going to target me? It's not really a defensible argument though. There are lots of people out there with time on their hands and lots of spare cycles on their computers, ready to see what mischief they can cause. And if you want to know more about what's possible, there's a scary story on *Ars Technica* at tinyurl.com/cf6neq9 that goes into the issues more deeply.

So, every day it becomes a little more likely that no matter who you are, you might just get caught by the bad guys. It pays to be always on your guard: change your passwords regularly, make them as hard to guess as you can, don't use the same user name on different systems, and back up the data that you can't afford to lose.

Back to Mat Honan: he was able to get a great deal of his data back (tinyurl.com/9glkf2m), thanks to the efforts of a disk recovery company and a couple of thousand dollars. But don't let that stop you doing the right thing with your security.

What's a library for?

Noting that the story at tinyurl.com/9nonyho is a journalist's view of what a library manager is supposed to be saying in a paper that hadn't yet been published, I'm just a little surprised at the generally defeatist attitude reported here. What I think he's saying is that libraries have a lot to offer the world of open data because they'll be giving their patrons internet access – either through library computers or wi-fi points. If this is so, I see it as a wasted opportunity to assist in information provision – and don't forget that you can get plenty of wi-fi access at McDonalds. I think public libraries would be better served by bringing their expertise to the challenge of guiding people to the sources of information and helping them to interpret it in ways that are useful to them. Or maybe they can just sell hamburgers.

Opening up

It's been a good week for the Open Government Data movement in Australia. First, the Victorian Government Data Directory at www.data.vic.gov.au was relaunched and then the ACT Government's Data Portal went live at data.act.gov.au. Having worked for some months on the ACT system, I have an idea of what goes on behind these systems – and it can get pretty complicated. We can try to get the data publication

process as automated as it can be, but there's usually a huge amount of work in identifying, checking, cleaning, and reformatting the data before it can be published in a form that brings credit on the organisation. The important thing is to share our experiences so that each iteration of the concept continues to improve.

How the cookies crumble

It started with a simple question in one of my groups: a member had followed a link to a website and then left without signing on or providing any obvious information about himself. A couple of hours later he received an email message from the site thanking him for his visit and advertising a free offer. He was a little confused and asked the collective mind how this could happen, because if a site writes a cookie to your browser, it can't access the rest of your computer – so where did it get the email address? After a couple of fanciful suggestions from people who thought they knew the answer, the truth was revealed: the site uses a third party service (herein called the Spam Facilitator) which writes its own cookie on the user's computer and then uses this to check to see whether the user has registered with any other of their clients. Any data that's been collected can then be shared by the Spam Facilitator with anyone else who signs up for their service. The good news is that you can protect yourself from this sort of practice, and it's quite easy to implement: see www.bobulous.org.uk/misc/third-party-cookies.html