Hiding in plain sight

by Danika Marquis

Being technologically savvy and secure is essential, and the unwary are likely to be targets of anything from phishing schemes, where their banking details are compromised, to being fired for posting objectionable messages on social media. However, there is the line between good practice to ensure your important information is safe and paranoia, which is likely to get you noticed by international governments for suspicious behaviour.

On 11 May 2014, the Guardian published an article on how one person's attempt to stay anonymous on the internet alerted the NSA to her actions. In this case, the person had an excellent reason: she was pregnant and did not want to deal with the plethora of internet browser adverts and emails targeted at new mothers.

For the uninitiated to the workings of companies like Google and Facebook, you may have been surprised when, after receiving an email invite to a wedding or baby shower, every advert you received on your browser and in your email for the next few weeks showed you hundreds of places to shop for suitable presents. This isn't magic, it's targeted adverting, which can, in some cases, be a wonderful and useful perk of internet.

The business model of companies like Yahoo, Facebook and Gmail allows users 'free' access to email and social media websites in return for company access to the gigabytes of information you store with them. This isn't as sordid as it sounds – I doubt a single individual is sitting at Google reading through my private messages (IMs and emails) and laughing right now about something stupid I wrote to my boyfriend at age 12 – but there is programme scanning for keywords, such as "baby" and "wedding".

They then sell this information on to advertisers along with ways to contact you and, if you have given them this information through Facebook or elsewhere, the area where you live. That part can be a concern – how can you trust advertisers and other companies with your address and what other personal information is going out and to whom?

> My guide for good practice is simply ensuring that your banking details, residence and identification number are not visible to the public.

My guide for good practice is simply ensuring that your banking details, residence and identification number are not visible to the public. This means, ensuring that emails with that information are encrypted, and that your personal email cannot be compromised. For this, I use Gmail's '2-way verification system' to ensure that my email isn't hacked. This system asks users to input a password and a secure code, which is sent to your cellphone, before using an unfamiliar computer to access your email.

In addition, any time I use my credit or debit card online, I ensure that the page on the browser I am using is secure ("https" rather than the less secure "http"). I also ensure that I don't broadcast my home address on Facebook and likewise that information and my identity number are not on any online CVs that I have posted.

But where is the line between healthy safety measures and paranoia? That is hard to place. It is a concern that governments use the same tools as Google and Facebook to spy on their own people, and likewise show an interest in communications with certain keywords. In the related article, Thomas Shone discusses that issue and how you can get around it, and he makes several valid points, but as noted above, sometimes our best efforts to ensure we are secure actually get us noticed quicker than if we just hid in plain sight – another face in the crowd on Facebook.