7 simple ways to avoid identity theft

One in four Australians report having been a victim of identity theft, and in 2015 59% of fraudulent credit applications in Australia involved identity takeovers. These figures tell us that identity crime is prevalent here, and I thought it well worth discussing, in particular what we can do to reduce it.

High value individuals can expect criminals to use a focussed strategy of home invasion, dumpster diving, social engineering, social media spying or hacking to steal identity details ranging from dates of birth, addresses, bank statements, credit card details, tax file numbers, passport numbers, or driver's licence details.

Criminals don't hang around once they've obtained high value IDs, and quickly gain access to a number of benefits in your name. Criminals will apply for loans, rent premises, apply for passports and submit tax returns in a victim's name. Victims usually find out about the breach when they try and apply for new services such as loans, medical benefits, passports, credit cards etc. and discover that they have been compromised in one or more of these areas.

Some even make the discovery when they lodge a "NOTICE OF INTENDED MARRIAGE" form, only to discover that they are already married to a complete stranger (usually a function of citizenship fraud). These and a host of other nightmares await victims of identity theft. In many cases it can take up to 18 months to get your life back. Follow a few simple strategies to avoid ID theft.

Let's start with physical security:

1. **Don't travel around in your day-to-day with important documents.**
   Originals of passports, birth certificates and social security cards should be locked away at home, or better yet in a safety deposit box or safe.

2. **Destroy all copies of important original documents such as contracts, IDs, passports and birth certificates etc.**
   Dumpster diving might sound like something out of a mediocre TV show, but if you are seen as a "high value" individual you may already be on an identity thief's radar – they know where you live.

3. **Personal information on USB sticks is a No-No**
   USBs are small, and can easily be lost. We are also often too cavalier in who we give them to, and can also forget what's on them. We hand them over to photo printing shops, your company's IT guy, casual acquaintances and colleagues too easily. Even our kids are likely to leave them lying around or lend them to friends. As an aside, always run a virus scan on any USB stick you need to use that belongs to someone else.

4. **Avoid doing phone or online banking in public.**
   Shoulder surfing and eaves dropping can often yield a wealth of personal identity information. Thieves can even use concealed long range cameras to record your details.

Digital Security

5. **Never, ever, ever click on a link in an email – it's as simple as that!**
   Every year over 10 million people are victims of phishing attacks. An example is unrecognised newsletters sent via email making you think you subscribed to the sender. These emails can contain a malicious "unsubscribe" link. If you don't recognise the subscription – then delete the email without clicking any links.

6. **Install security software on your phone**
   This is a critical weak point in most people's digital security. Most security packages have a multi-device option, use one of these licences on your phone. We forget how much info we communicate over apps and mobile. See more on Mobile Device Security on our web site at: https://onlinedigitalsecurity.com.au/software.htm

7. **Embrace Biometrics**
   Any time your bank or another institution begins a biometric programme, embrace it. Biometrics uses finger print, iris and facial recognition software to identify people, and is an excellent way of combatting identity theft.

You, as a person, are unique and full of nuances and characteristics that make you immediately identifiable to loved ones and friends. However, when it comes to government and large institutions, for reasons of practicality and scale, you are simply a collection of data points. This means those sets of numbers are valuable, but also replicable. Keep them close.

By Johann Koelmeyer (CEH) - Cyber Security Engineer at https://onlinedigitalsecurity.com.au

ODS
Online Digital Security
Your trusted defence against Cybercrime