safe community

by David Thomas

features@algarveresident.com

David Thomas is a former Assistant Commissioner of the Hong Kong Police, consultant to INTERPOL and the *United Nations Office on Drugs and Crime*. In October 2011 he formed *Safe Communities Algarve* an on-line platform here in the Algarve to help the authorities and the community prevent crime.

# Stealing your identity

I always remember watching a Sci-Fi film a few years ago entitled *Star Trek - Nemesis*, where Captain Picard is cloned; in this case creating a criminal "double".

Implausible? Possibly not in the case of identity theft.

Identity fraud is something that occurs when your name and personal information is used by someone else, without your knowledge, to obtain goods, credit or other services fraudulently.

This can result in someone securing official documentation, including a passport in your name – scary, isn't it? So the aim of this article is to show you how to avoid fraudsters obtaining your information and thus reduce the risk of fraud.

Placing a statistic on identity fraud is difficult but research in the USA, conducted by Javelin Strategy and Research, found that in 2011 some 11.6 million US adults were victims of identity fraud.

A survey in the UK found that 7% of people have been victims of ID fraud – one in two of whom has lost money as a result, with the average amount lost being £1,190 per victim.

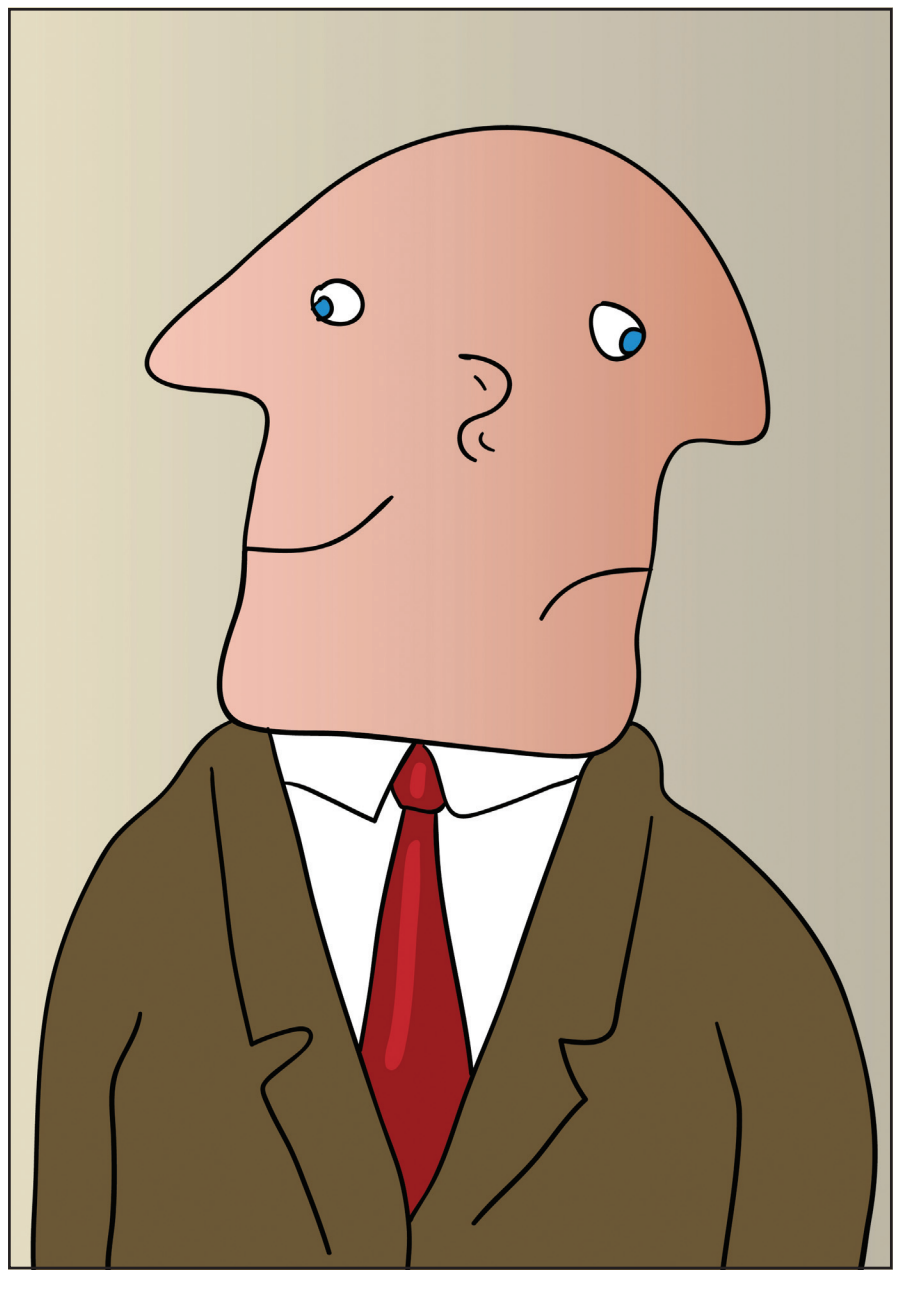
I can find no figures for Portugal. However, given that "identity theft" recognises no borders, I am sure that this type of crime is rising. In one example, a couple were buying a house in the Algarve and applied for a mortgage only to be told a bit further down the line that they were blacklisted in the UK (whilst living in Dubai at the time). When they found out details of the blacklisting, someone had applied for an American Express card in the husband's name and run up a bill of £11,000 pounds and not paid.

The US survey identified certain social and mobile behaviours that had higher incidence rates of fraud than all consumers. LinkedIn, Google+, Twitter and Facebook users had the highest incidence of fraud although there is no proof of direct causation. The survey found that despite warnings that social networks are a great resource for fraudsters, consumers are still sharing a significant amount of personal information frequently used to authenticate a consumer's identity. Specifically, 68% of people with public social media profiles shared their birthday information (with 45% sharing month, date and year); 63% shared their high school name; 18% shared their phone number and 12% shared their pet's name - all are prime examples of personal information a company would use to verify your identity.

This is born out in the UK whereby a survey found that 88% of people who use social networking sites have shared items of personal information online that could be used by ID fraudsters, including sensitive information about other people.

## How your identity can be stolen

There are many ways that someone can steal your identity, including finding out your bank details; taking your passport or driving licence, or copying the details; copying your credit card details; accessing your personal information through a fraudulent website or email; taking junk mail that has your personal information on it and going through your dustbin to find receipts or other information. You may not know straight away that your identity has been stolen.



## How to reduce the risk of identity fraud

Firstly, of course, is to be vigilant; be very cautious of anybody who contacts you unexpectedly (by phone or through email etc) and asks for personal information or account details even if they claim to be from the authorities or your bank. Ask for their name and a contact number and then check with the organisation in question before calling back.

It is important to guard your credit cards. Minimise the number of cards you carry in your wallet. In particular do not carry a written pin number with you. If you lose a card, contact the fraud division or emergency contact number of the relevant credit card company. If you apply for a new credit card and it doesn't arrive in a reasonable time, contact the issuer. When you receive a new card, sign it in permanent ink and activate it immediately. Watch cashiers when you give them your card for a purchase and make sure you can see your credit card at all times. .

**Shred all documents** – Shredding documents is the best way to ensure that criminals cannot build up a profile based on the information you discard in your rubbish. Invest in a powerful cross-cut shredder and make it a standard practice to shred all documents containing personal or financial information before binning or recycling them.

**Keep your documents safe** – Store any documents containing personal details, such as your passport, driving license, bank statements or utility bills in a safe place. In addition, limit the number of documents you carry around with you that contain your personal details. If possible, do not leave personal documents in your vehicle, except those required by law.

**Secure your post** – If you use a central or communal postal delivery point, make sure your mail is secured until you can collect it. Consider a lockable post box and collect your mail as soon as possible.

> Invest in a powerful cross-cut shredder and make it a standard practice to shred all documents containing personal or financial information

## Being safe online

If you use the internet ensure you have the latest security patches and up-to-date anti-virus software installed. Social networks have gained enormous popularity in the last years. An excellent website www.getsafeonline.org offers advice on keeping your details private on social networks as well as other advice such as avoiding scams, phishing attacks etc. You can avoid the risks and enjoy social networking sites by following a few sensible guidelines in particular:

- Don't let peer pressure or what other people are doing on these sites push you into doing something you're not comfortable with. Just because other people post their mobile phone number or birthday doesn't mean you have to.
- Be wary of publishing any identifying information about yourself. In particular things like phone numbers, pictures of your home, workplace or school, your address, birthday or full name.
- Pick a user name that doesn't include any personal information. For example, "Joe_albufeira" would be a bad choice.
- Use a strong password and not the same one for all websites.
- What goes online stays online. Don't say anything or publish pictures that might cause you embarrassment later.
- Learn how to use the site. Use the privacy features on the site you use to restrict strangers' access to your profile. Be guarded about who you let join your network.

The Polícia Judiciária (Judicial Police) has issued a number of Citizen Alerts over the last few months concerning phishing, online fraud and credit card fraud. Two excellent preventative guidelines, entitled "Prevention of Credit Card Fraud" and "Protecting your Computer Against Social Engineering Attacks", both issued by Europol, can be found under Crime Prevention Advice and Downloads on the Safe Communities Algarve website, www.safecommunitiesalgarve.com.

■ *David Thomas, Founder of Safe Communities Algarve can be contacted at 913045093 or by email at info@safecommunitiesalgarve.com. More about Safe Communities Algarve can be found on its website www.safecommunitiesalgarve.com*