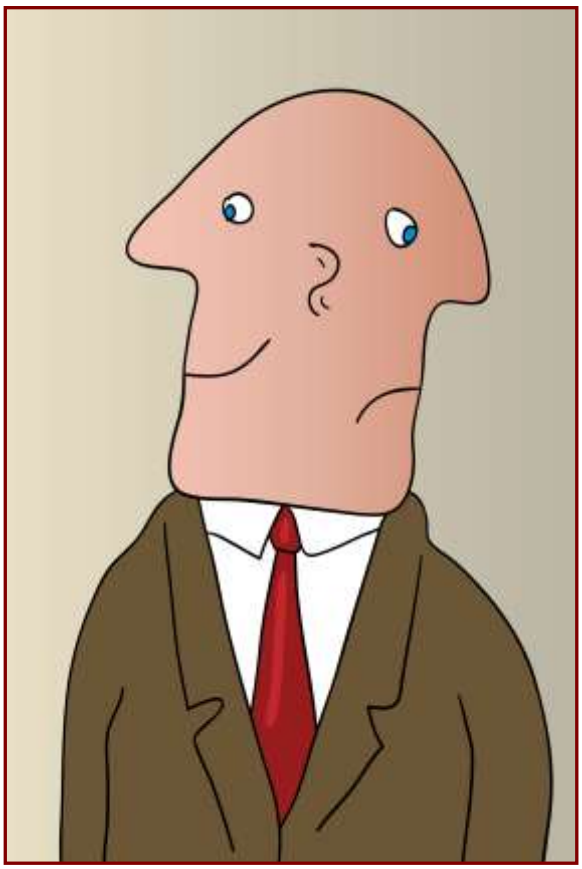
# Have you been cloned?

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.

**Data Breaches**



From ordering food, requesting a taxi and checking our bank accounts, to meeting new people and selling our unwanted items, more of our lives are spent online. And whilst these digital services have given us more convenience and a better customer experience, we are giving our personal data to an unlimited number of people and companies.

And we’ve lost track of the details we’ve given – after giving them to so many different people and companies, it’s hard to remember who we gave our details to, what information we gave or when we gave them. A terrifying thought when news of data breaches hit the headlines almost every day.

In fact, in 2016 alone a record 421 billion data records were stolen. If that’s not scary enough, 35 data records are stolen every second and over 3 million data records are lost or stolen every day.

**Identity theft and fraud**

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

Placing a statistic on identity fraud is difficult, but According to Javelin Strategy, the number of identity theft victims in the US rose to 15.4 million in 2016. The cost of all of that lost data amounts to $16 billion.

Identity theft has reached epidemic levels in the UK, with incidents of this type of fraud running at almost 500 a day. During the first six months of 2017 there were a record 89,000 cases of identity fraud, which typically involved criminals pretending to be an individual in order to steal their money, buy items or take out a loan or car insurance in their name

I can find no figures for Portugal. However, given that “identity theft” recognizes no borders, I am sure that this type of crime is rising.

Specifically, 68 percent of people with public social media profiles shared their birthday information (with 45 percent sharing month, date and year); 63 percent shared their high school name; 18 percent shared

their phone number; and 12 percent shared their pet's name - **all are prime examples of personal information a company would use to verify your identity.**

In the UK 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 you 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 off course is to be vigilant; be very cautious of anybody who contacts you unexpectedly (by phone or though 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. Watch cashiers when you give them your card for a purchase and make sure you can see your credit card at all times.

.

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.

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.

## Being Safe On-line

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 on-line. Don't say anything or publish pictures that might cause you embarrassment later.

- 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.

More details on this can be found on our website www.safecommunitiesportugal.com

David Thomas
President
Safe Communities Portugal

6th April 2018