Protect yourself from Identity Theft and Fraud

Personal Information

Posting personal information on the internet can lead to unwanted attention – including identity fraud. Social networking sites in particular allow you to post detailed, personal Information about yourself, from your date of birth, to all the schools you went to, to your favourite film: precisely the information that banks ask for as security questions. Be careful about making the following information publicly available:

- **Your full name**
- **Your full address**
- **National insurance number**
- **Date of birth**
- **Telephone number**
- **Postcode**

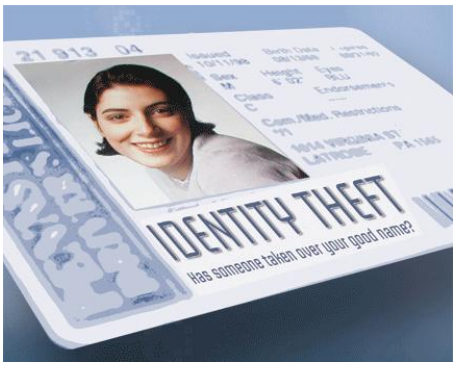
And if you're asked to provide to this information, always ask yourself the question: 'why am I being asked to provide this information / make it publicly available?'

Fraudsters

Potential fraudsters can take seemingly random pieces of information about you from a range of sources that allow them to take guesses at bank security questions; build up a profile of you which allows them to impersonate you; to open up credit cards in your name or to get access to more of your personal information.

Security Questions

Our advice is don't make the following information publicly available either:



- **Mother's maiden name**
- **Current place of study**
- **Current employer**
- **Birthplace**
- **Recent addresses**
- **Recent places of study e.g. last school attended**
- **Details of your interests e.g. pet's names, favourite film, favourite colour**

And always be suspicious of anyone who asks for your:

- **Bank account details**
- **Credit card details**

… or you could fall victim to phishing (see E-mail leaflet)

Facebook

A recent 'sting' carried out by the IT security company Sophos on Facebook, found that 41% of people would enable a complete stranger to see their profile, potentially allowing them to see personal information.

(http://www.sophos.com/pressoffice/news/articles/2007/08/facebook.html)