How ID Fraud Works: At Home

BIN RAIDING

Fraudsters pay people to go through the rubbish you throw out, looking for bank and credit card statements, pre-approved credit offers and tax information. Everyday information that you may not think is important such as old gas, electricity and telephone bills, insurance documents, bank statements and even personal letters carry valuable personal information that can be gathered together to steal an identity.

A bin raiding survey commissioned by Fellowes for National Identity Fraud Prevention Week showed that an alarming 79% of household waste contained at least one or more items which could assist fraudsters in stealing an identity. Even more worryingly, almost half of all households threw away everything a potential fraudster would need to steal a person's identity.

MAIL FORWARDING

By not asking Royal Mail to redirect your mail when moving house, fraudsters can receive a wealth of information about you delivered direct to their doorstep. Visit www.royalmail.com for more information.

UNSOLICITED CONTACT

Phone calls claiming to be from banks asking you to update your personal information should be regarded with caution. Calling the switchboard of the company in question and asking to be put through to the person who called you will help ensure you are not playing into the hands of fraudsters.

Similarly, fraudsters posing as market researchers may ask for personal information over the phone. Credible organisations will not mind you double checking their authenticity before providing such information.

ONLINE

PERSONAL INFORMATION ONLINE

Anybody that uses the internet will regularly be asked to share personal information to gain access to websites and buy goods. Increasingly people are also placing large amounts of personal information about themselves on social networking sites such as Facebook, Bebo, Twitter, Linkedin and MySpace.

It is worth mentioning that date of birth, address, full name and place of birth will often be enough to get someone's identity stolen; now check your Facebook page and ask how much of that information you're sharing with anybody who'd care to ask.

Fraudsters can combine the personal information you provide to unsecured internet sites such as your mother's maiden name with other bits of valuable information they glean about you to obtain credit in your name.

PHISHING

This term describes identity theft via email. Fraudsters will send an email claiming to be from a bank, a credit card company or other organisation with which you might have a relationship, asking for urgent information.

Typically the email will ask you to click on a link to enter your account details on the company's website to protect against fraud or to avoid your account being deactivated. But if you click on the link in the email you will be taken to a website which looks genuine but has in fact been created by fraudsters to trick you into revealing your private information. The fraudsters then use the information provided to set about obtaining money from your accounts.

WHEN YOU ARE OUT

THEFT OF WALLET AND PURSE

The average purse or wallet contains bank cards, credit cards and valuable identity documents including driving licenses and membership cards. Victims realise very quickly that their wallet has been stolen but often do not realise the value of the information contained within it until it is too late.

CARD SKIMMING

This usually occurs when a shop assistant or waiter, for example, gets your information by 'skimming' or copying your credit card information when you make a purchase. They often then sell the information to professional criminal gangs. Like phishing, skimming can be used on its own to collect enough information on your credit card to use your card fraudulently without stealing your entire identity.