ARE YOU BEING CL

Wake up to the shocking facts about ID theft during National Identity Fraud Prevention Week...

Celebrities aren't the only ones who are worried about strangers taking an interest in their bins. Thanks to all the warnings about identity fraud in the last few years, most of us know it's asking for trouble to throw away bank and utility statements without shredding them first.

It's a hassle but saves you sorting out the mess if someone steals your personal details and racks up huge bills in your name.

But despite the fact we're more aware, identity fraud scams are getting ever more sophisticated – and more frequent.

The internet is the main problem. Online ID fraud has emerged as one of the fastest growing crimes, and over a quarter of us have been a victim or know someone who has. It ranges from relatively small amounts of a few hundred pounds to having credit cards or even mortgages taken out in your name, or your driving licence or passport cloned.

It's big business. According to research by online fraud experts Garlik, the average consumer's identity could be worth as much as £85,000 to thieves.

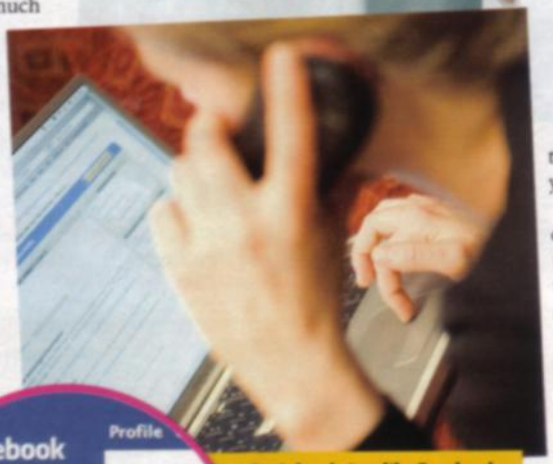
'The new growing breed of ID thieves has moved on from rummaging around in bins,' says Garlik boss Tom Ilube. 'Rather than scouring the streets for personal information, they spend hours surfing the web building up a full identity profile to sell on.'

One reason it's getting worse is that documents that were once only available on request are now online. Marriage and birth records can be seen on genealogy websites, and planning applications on some local authority sites sometimes, amazingly, include a scan of a signature.

Most recently it emerged that criminals were searching social networking sites like Facebook and MySpace. Personal details posted by people, such as their date of birth or school, are a godsend to thieves, as this is the kind of information banks use as security questions. 'Everybody's got to become more aware of the kind of information they're sharing,' says Tom Ilube. 'If you include your date of birth, email address and postcode, with links to your mother and partner's pages, you're making it very easy for thieves to guess your passwords.'

The other common scam is 'phishing', where you receive an email trying to trick you into giving personal details. The number of bogus emails rose from 1,700 in 2005 to 14,000 last year.

'The really sinister thing about these emails is that they're designed to scare us,' says Anna Fielder of the National Consumer Council. 'They often talk about internet security being breached and encourage us to click on links within the email. Never, ever go to a website through a link in an email because you might end up with spyware on your computer, and that would mean that hackers could read all of the documents on your computer, and easily steal your identity.'

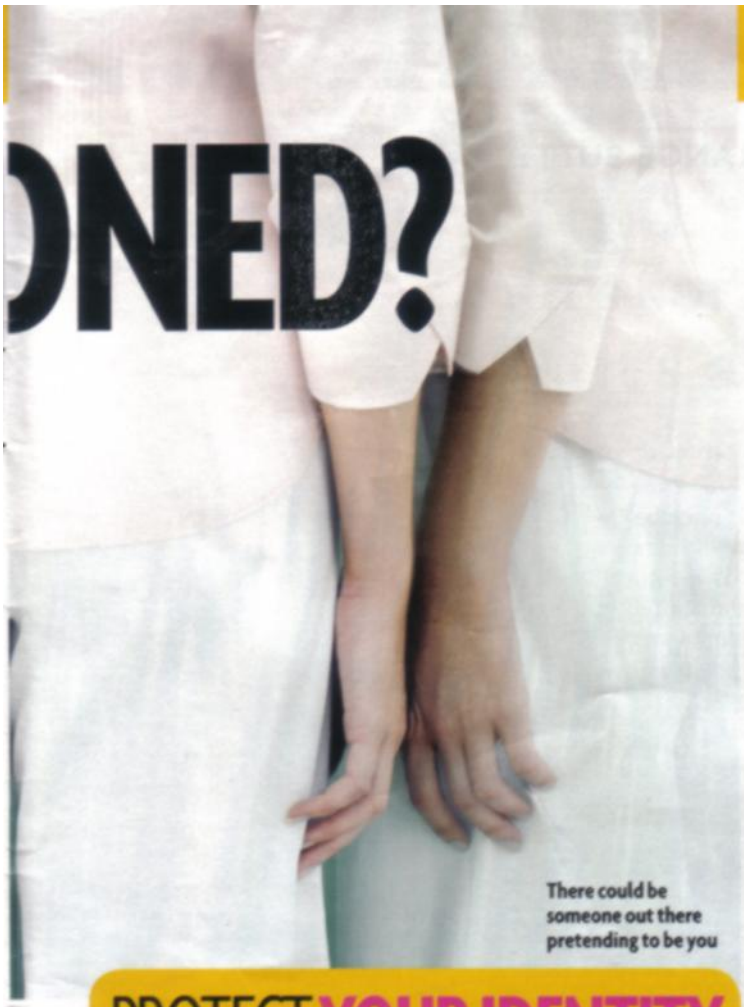


Social websites like Facebook, left, can be a dream come true for internet fraudsters

HOW WIDESPREAD IS ID FRAUD?

- Over 170,000 cases of identity fraud were reported in the UK in 2006 – up nearly 13% on the previous year.
- The Home Office says that identity fraud costs Britons around £1.7 billion a year.
- Online ID fraud is part of a worrying growth in internet crime, which affects one of us every 10 seconds.
- Credit card details are being sold on to thieves for as little as £1, with a person's full identity on offer at £10.
- The average amount stolen in identity theft cases is £6,000 but can be anything between £1,000 and £30,000.

ONED?



There could be someone out there pretending to be you

PROTECT YOUR IDENTITY

Neil Monroe from credit reference agency Equifax reveals how to dodge the identity thieves.

- Don't reply to emails that appear to come from banks, credit card or other trusted companies asking you to update your security information.
- Always type website addresses into the browser yourself – never click on email links.
- Don't enter personal or financial information unless the web address starts with https:// and there's a small padlock in the browser window frame. The 's' signifies that it's secure.
- When you move home, make sure you have your mail redirected to the new address.
- Make sure your PINs and passwords are all different, and don't use obvious things like your birthday or phone number.
- Always check bank and credit card statements against your receipts. If you find any unfamiliar transactions, contact your bank or credit card company immediately.
- Check your credit report frequently – the most effective way of identifying identity fraud. Contact Equifax on 0870 010 2091, www.equifax.co.uk, or try Experian on www.experian.co.uk.

Don't ever enter your credit card details on an unsecured website

Words Yvonne Govan Photos Alamy, Getty, Mark Ferguson

'I WAS A VICTIM OF IDENTITY FRAUD'

Ros Holdsworth, 41, lives in Falkirk, Scotland. She is married with a 15-year-old daughter.

After a weekend away with my husband, I was on a high as I went to work one Monday in 2004. But I got a real jolt when I checked my bank account.

'The balance was £1,000 less than it should have been. I flew into a panic as I had some big bills coming out that day.

'At first, I thought I'd massively overspent, but when I went through the transactions on my online statement, I saw three big debits had been made for things I didn't recognise.

'One of them was a £300 bill to Orange for a mobile phone. When I called them, they said I'd ordered the phone the Friday before and asked for it to be sent to an address in Hull.

'I felt sick, knowing someone had pretended to be me and stolen my hard-earned cash from under my nose. But I didn't have a clue how they'd done it.

'I called my bank, The Royal Bank of Scotland, to explain, and they told me to come in straight away. I was terrified they'd think I was making it all up.

'They shut down the account and opened up a new one in my name. But I had to sit through a meeting with the bank manager asking me loads of questions, like when I'd last used my account and if anyone else knew my password. Even though they were being helpful, I broke down in tears because it felt as if I was being interrogated for something I hadn't done.

'I was told that the biggest single payment they'd made was £600. Through a bit of detective work of my own, I discovered that this amount had been used to set up a new website.

Ros still doesn't know how her money was stolen

'I passed on all the information I had – my receipts from Orange and the name of the company that set up the website – to the police. I was determined someone should be prosecuted.

'The irony is, I'm very careful with money. I check my account every day and keep my receipts.

'The bank gave me an overdraft to cover the missing money, but it was four months before they actually refunded it. They haven't caught anyone, and I still don't know how it happened. It could have been when an internet transaction went wrong and I had to call and give details over the phone. That can be risky, but you just trust people, don't you? Well, I certainly don't any more.'

'£1,000 had gone from my account'