



ID THEFT

Did you hear about Sidney Davids?

He was a good friend of ours but, alas, Sidney Davids became a victim of ID theft... And now his name is Sney Davs. Tragic. Not that that's the very worst thing that can happen. Not that it's true, either. Nevertheless, here's an Info Sheet to tell you what you can do to reduce the chances of ID theft happening to you...

We've never had it so good...

We've never had it so good... Back in the day when we had good, wholesome honest crime, a lost or stolen wallet meant chummy did the naughty and got a few quids' worth of stuff, the police tsk-tsked and put you onto the banks, the banks explained it was a terrible thing and privately complained they had to pay for it... You, meanwhile, had to work out what you didn't spend and claim it back. These halcyon days are long gone!

Now, if you've lost your wallet or purse, it can be the start of something much larger and more insidious. Do report lost or stolen property to your local police immediately, using a non-urgent number, or pop in to the station if you'd rather. Some constabularies are set up to take reports of lost property online! It may show up and, even if it doesn't, it could make things easier in the event that ID theft becomes your problem. Keep a copy of the crime number if one is issued.

You would cry too if it happened to you!

Before we look at what to do to prevent ID theft, let's take a shufti at how on earth you'd know if someone did steal your identity! There are several clues, including:

- Post that you're expecting from your bank or building society doesn't arrive or the amount of post that you receive drops suddenly
- You get post that you aren't expecting – a letter from a solicitor, for example, or debt collector demanding money for a debt that isn't yours
- Things appear on your bank statement that you can't account for
- You apply for some kind of benefit and are told you're already getting it!
- You believe you have a good credit rating but are refused a loan or other financial service

It might also be that you're about to become a victim of ID theft if you've lost, or had stolen, any bank statements, National Insurance details, a passport or driving license.



Check out the moves:

One good way to ensure that your bank, credit-card company and other relevant parties don't unwittingly help criminals is to make sure you tell them you're moving... Twice. Do it once verbally, then do it again in writing. It's also wise to get, within a couple of months of moving, a copy of your credit file...

When you do move your house or business, it can be worth paying Royal Mail to redirect your post for at least a year. It costs in the region of £40 for a residential address and £80 for businesses, which sounds a lot... But is a trifling sum in relation to the cost and distress of being a victim of ID theft!

"Lots and lots of files..."

In fact, it's a sensible idea to get a copy of your personal credit file quite routinely. They cost a few pounds at their most basic; check yours through to see if it has an entry that doesn't ring any bells.

Gone phishing:

Very much a modern guise of an old idea, 'Phishing' is a scam designed to get you to part with sensitive financial information via email. Usually, an email unexpectedly appears from what seems to be your bank. It asks either that you click on a link and enter account details on their site, or that you reply to the email and confirm some account details.

It shouldn't surprise you to learn that the email and site are both fake, yet people lose millions of pounds through these scams year in, year out! They can be very convincing, so you need to remember one thing: **NO** reputable financial organization uses email to discuss sensitive account information. Ever. If you have any kind of email from 'your bank' and you're reluctant just to hit delete, then simply call them to see if it's real... Using a telephone number from a source other than that email, of course!

What's good for the goose:

So 'Phishing' is an email based technique designed to persuade you to part with information that allows ne'er do wells to steal your money, identity or both. And there are dozens of versions of that sort of thing! So rather than explain each one, you might choose to visit the site that keeps track of many of the best, worst and most prevalent - <http://www.hoax-slayer.com>.

"You are number six..."

If you're particularly concerned to stay ahead of identity thieves, you might want to register with the Credit Industry Fraud Avoidance System. A number of financial organizations have joined CIFAS and now undertake more stringent checks against your name, once you've registered it, to ensure applications are legitimate and verified more thoroughly. This makes it much harder for anyone to use your details if they get their sticky little mitts on them.

Say it, say it, say it again now!

You know how it is when you order something over the phone: the person taking your details repeats your credit card number to make sure they've got it down right, right? Right! But the fact is they often do it surrounded by other people, none of whom you know and any of which can jot it down and use it! So politely suggest that, instead of them repeating the number, you'll say it twice instead.



The Teenage Mutant Hero Turtles

found having a shredder around caused no end of trouble. But they're in a minority. Since most business records have privileged information on them, they're ripe for the picking! Shred all your old records or have a reputable specialist do it for you.

Harry Hou?

Harry Houdini was a master lock picker... In his 35 year career as a magician and escapologist, he never failed to pick open a lock of any kind. He was a rare one, though! Truth is most criminals are more likely to use a brick than a pick!

So this is a simple tip: store any paper files you do have in a locked filing cabinet. Do so at home as well and, in the same way, keep any electronic records that you have on physical media secured and make sure your computer accounts are password protected.

What's the magic word?

Keep any access and online passwords that you have, to yourself and try to avoid writing them down if possible. It can seem a bit daunting to do that, but several people we know use a system that combines the name of the site they're on with one very difficult to guess – but easy to remember – password!

On no account store passwords on your phone or in your wallet, handbag or purse.

Who ya gonna call?

Be tremendously cautious about giving out any information to people, especially over the phone and remember: those legitimately asking for essential information will certainly understand caution on your part. In fact, as long as you're polite, they often appreciate it. Finally, only give your credit card number on the phone or voicemail if you trust the person or company you're dealing with; never email them or use a site where the payment system looks dodgy!

If you receive a call and have some doubt about who's on the line, explain that you'd be happier if you called them back. Take a number down and then confirm it's legitimate using a different source. If it all sounds a bit fishy, ask how the info is going to be used, for what and by whom. It's quite reasonable to ask what measures people have taken to ensure your details are protected.



En garde!

Prepare for the worst as you type in Personal Identification Numbers and passwords. Try to shield the keypad as best you can and, if you're stood at an ATM, do check it over for signs of tampering. We'll be doing an ATM fraud Info Sheet in the near future... Meanwhile, try to use machines you know are real, look for some distinguishing marks on the keyboard and card slot, and check that they are the same before you use them.

Never too late:

If you are the victim of ID theft, make sure you:

- Report it to the police
- Keep details of the things you do to put the matter right – and the cost of those actions
- Close your bank accounts and open new ones; cancel your credit cards and get new ones issued... Be sure to tell the bank or building society what's happened, ask for up to date advice
- If your passport or driving license has been stolen, tell the relevant party immediately
- Ensure your credit report reflects the identity theft
- Check your report again, three and six months later, to ensure that no-one's tried to use your identity since
- Call your phone, cable television and utility companies to advise them that your name could be used to open a fraudulent account