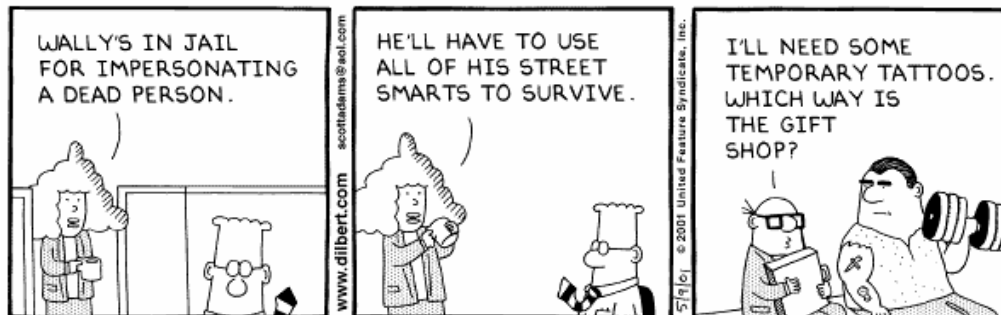


Chapter 6 - Identity Theft

Once again Wally is the brunt of the Pointee Haired Manager's stupidity and he is finding out to the hard way that impersonating anyone for the purposes of fraud is a serious crime. And that is exactly what Identity Theft is – fraud.



Copyright © 2001 United Feature Syndicate, Inc.
Redistribution in whole or in part prohibited



Copyright © 2001 United Feature Syndicate, Inc.
Redistribution in whole or in part prohibited

Identity theft or identity fraud as it is sometimes known is ubiquitous and growing in an epidemic proportion. It is also a very personal, and sometimes life destroying, crime.

In the UK, the Home Office estimates that it costs the economy billions of pounds each year and is on the rise. The national price tag for fraud has increased from £1.3 billion in 2002, to £1.7 billion in 2004, and in 2006 nearly £2 billion per year,

However for the average individual it is not only the cost but the huge amount of time and stress it takes to rectify. In many cases victims find that:

- They are forever refused credit applications, as they have been left with a bad credit rating.
- They are sent constant letters about debts that they did not run up.
- They incur legal fees and sometimes even have to work to have criminal convictions quashed.
- And in the worse case can be refused Visas or even jobs, where a background check is required.

People don't listen!!

There is a huge body of people who claim that it is all a conspiracy to make life difficult. They refused to face the facts, even though they are overwhelming. And unfortunately, they encourage people to follow their own irresponsible example. Years ago, people who lived in villages and even large towns felt that they did not have to lock their front doors-but through learning the hard way, by facing up to modern times, these same people have learnt to double bolt and deadbolt their front doors to stop them being victims. And so it is with ID fraud, as Clarkson can demonstrate.

The Jeremy Clarkson story

Jeremy Clarkson is every boys, mine and Dilberts' hero for his lad-ish, high-bravado style. Recently, he joined the ID_THEFT_IS_ALL_A_MYTHE gang and published his bank details in his newspaper column, rubbishing the idea of identity fraud - A real *I dare you*. He was soon amusingly proved wrong as one cheeky wag set up a direct debit for £500 per month from his account to a diabetes charity. Below is how it was reported on the BBC website.



- [News Front Page](#)
- [World](#)
- [UK](#)
- [England](#)
- [Northern Ireland](#)
- [Scotland](#)
- [Wales](#)
- [Business](#)
- [Politics](#)
- [Health](#)
- [Education](#)
- [Science/Nature](#)
- [Technology](#)

Entertainment

Also in the news

- [Video and Audio](#)
- [Have Your Say](#)
- [Magazine](#)
- [In Pictures](#)
- [Country Profiles](#)
- [Special Reports](#)

- RELATED BBC SITES
- [SPORT](#)
 - [WEATHER](#)
 - [CBBC NEWSROUND](#)
 - [ON THIS DAY](#)
 - [EDITORS' BLOG](#)

Last Updated: Monday, 7 January 2008, 11:56 GMT

[E-mail this to a friend](#)

[Printable version](#)

Clarkson stung after bank prank

TV presenter Jeremy Clarkson has lost money after publishing his bank details in his newspaper column.



Jeremy Clarkson found himself unexpectedly donating to charity

The Top Gear host revealed his account numbers after rubbing the furore over the loss of 25 million people's personal details on two computer discs.

He wanted to prove the story was a fuss about nothing.

But Clarkson admitted he was "wrong" after he discovered a reader had used the details to create a £500 direct debit to the charity Diabetes UK.

Clarkson published details of his Barclays account in the Sun newspaper, including his account number and sort code. He even told people how to find out his address.

“ I was wrong and I have been punished ”

Jeremy Clarkson

"All you'll be able to do with them is put money into my account. Not take it out. Honestly, I've never known such a palaver about nothing," he told readers.

But he was proved wrong, as the 47-year-old wrote in his Sunday Times column.

"I opened my bank statement this morning to find out that someone has set up a direct debit which automatically takes £500 from my account," he said.

"The bank cannot find out who did this because of the Data Protection Act and they cannot stop it from happening again.

"I was wrong and I have been punished for my mistake."

Apart from the strange comment about data protection, (it is bank fraud after all,) the story explains the issue better than I could.

How do they do it

To understand how to deal with ID theft you need to understand how it is done - There are a number of basic types of identity theft:

Account takeover - is when a thief gains control of your **existing** credit cards or bank account information and using the actual credit card or simply the account number to make himself rich at your expense.



© Scott Adams, Inc./Dist. by UFS, Inc.

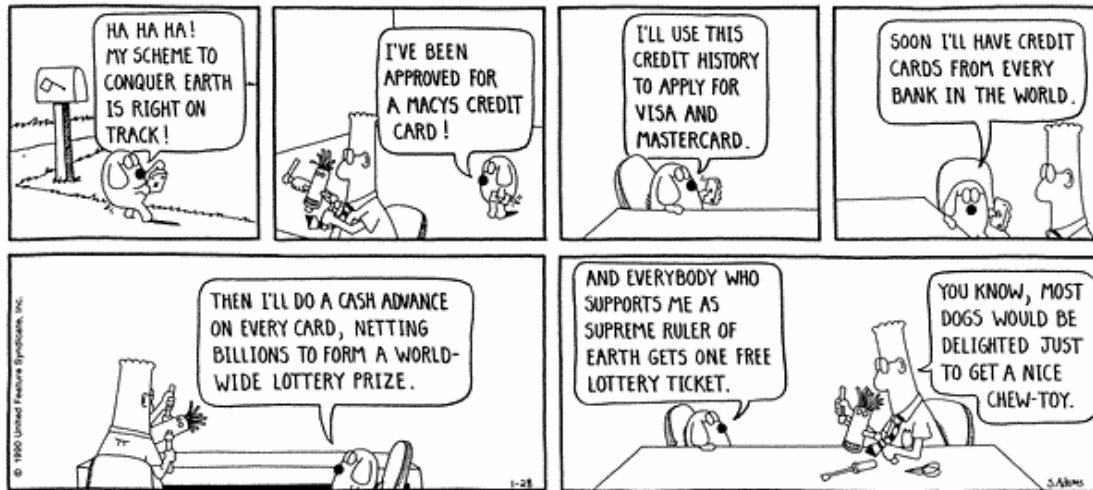
Dilbert has already covered many of the causes for this type of ID fraud. Dealing with insecure websites and/or organisations is a sure way to make sure bad guys get your credit card details.

If that isn't the cause, another common cause is "Card Cloning". This occurs when you let your card out of your sight and the vendor runs the card through a copying device. In the UK, the way this is done has changed because of the introduction of "Chip 'n Pin" cards. Here cards have a special microchip installed which is electronically bound to your pin number – without it the card is useless. Unless, of course, the villain makes purchases in a country that still uses old style non-chipped cards – like Australian, New Zealand or Mexico.

So that's what happens – they copy the information in the UK or Europe and send the info to Ausie where they make a copy of the card and rob you blind. Interestingly this transfer of fraud to a different jurisdictions is known in the card industry as F.A. – Fraud Abroad!!!

When you go to check your bill you find all sorts of expenditure that you never made. In my case it, a bogus \$800 was charged *To Mehimits Exotic Leather Goods* in Turkey – very hard to explain.

Application fraud – Here the bad guys use your personal information to open **new** accounts.



Sometimes called 'Name fraud' this can be very serious. Not just a few thousand pounds on a credit card, there have been reported cases of mortgages for houses and expensive cars extorted in this way.

Dogbert, above, shows exactly how it can be done. When you get a store debit card, the cashier opening an account will usually ask for:

- Two utility bills (gas or electric)
- A form of identification
- A telephone number
- Some bank account details

And that's all the bad guy needs to open a line of credit at your local white goods store – in your name. Order fridge freezers and wide-screen TVs on the account then just sell them on Ebay for cash.

The bad guy can gain this stuff if he has access to your mailbox, or he can use dumpster diving to gain it. The use of pay-as-you-go mobile telephones will allow the bad-guy to have a dialog with the credit company – there is no need to bother you. Any deposit can be provided by a credit card in your name by using a pay-as-you-go credit card – this will add creditability to the affair the clerk will probably not know the difference between the card types anyway.

Other information that a badguy can use to steal your identity is:

- National Insurance Number or social Security Number
- Education/Employment history - can help a badguy get a job as "You". Lets face it even if your new employer does bother to take-up reference, they will probably not send a photo of the applicant to the referee and ask him to confirm your appearance. It is surprisingly common to find people using other

peoples identities to gain temporary employment.

Let's face it one bald fat guy, looks remarkably like another. Should someone steal your driving license – they probably will sell it unaltered to someone who looks just like you.

Reports suggest The 'back from the dead' canoeist John Darwin Who turned himself in dec 07 created his new identity by obtaining a legitimate birth certificate, just like the villain did in Fredrick Forsythe's the Day of the Jackal. In the UK, birth certificates can purchased from the government on the Web.

How to avoid ID Fraud

Don't tell anyone your password

Don't tell anyone you password, or pin number or bank authentication code.



Your user ID and password digital world are the equivalent of your signature, and you would never sign a blank piece of paper or a contract or a cheque without reading it.

A corny slogan that I have been using for years “**Your password is like your toothbrush – You need one, you should change it often and you don't share it!!**”

Or your PIN, even if you are asked



Copyright © 1999 United Feature Syndicate, Inc.
Redistribution in whole or in part prohibited

Your PIN is another form of password – don't write it on the back of the card or tell anyone, or the banks will hold you responsible for any loss.

As general rule, you should never give any personal details to someone phoning you.

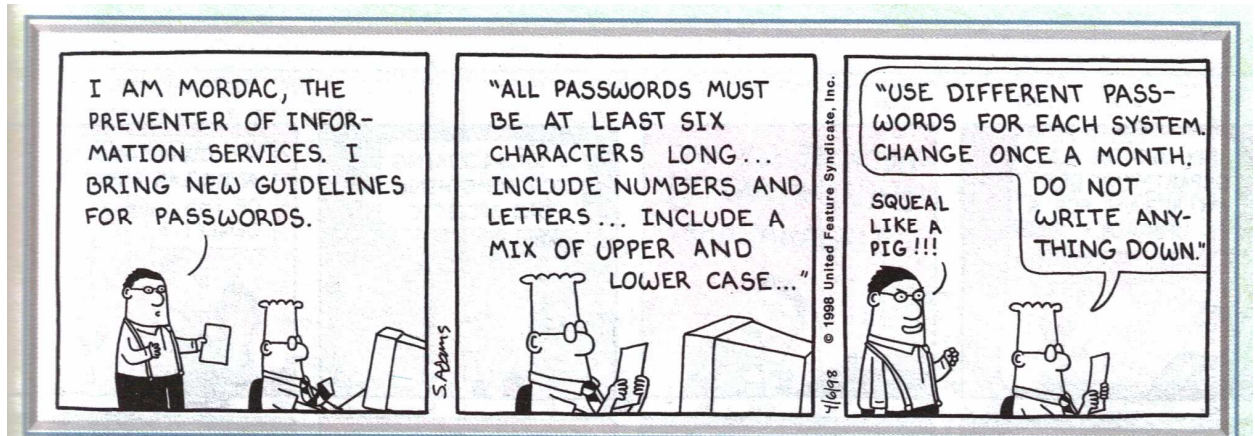
Choose an Internet Bank that uses Fancy security



Despite what I claim in the next tip, there isn't really such a thing as a good password – they aren't really a very good security device. For your Banking, use something much stronger like one of these hardware tokens.

Choose Good Passwords

When using an online system get into the habit of using a good password.



Mordac is enjoying Dilbert's discomfort above but really he is doing Dilbert a kindness. A password that doesn't change or can be guessed is next useless.

So use a password phrase or Hacker speak known as L337 (leet).

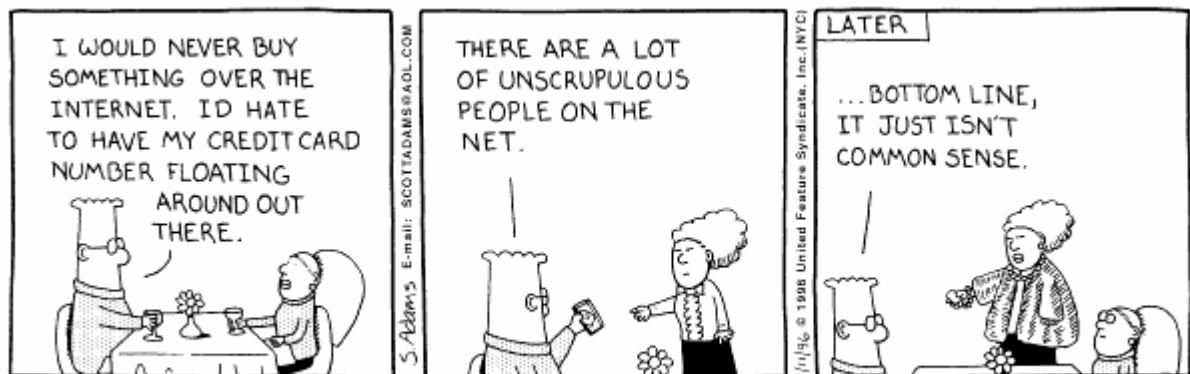
A password phrase is just a posh way of describing an ACRONYM that makes a long password easy to remember. So a password phrase of "I was 21 last January 13th" would produce a password of "Iw21J13" – easy enough.

Leet spells words out of Numbers, *symbols and letters* :-

- *St3v3n!* Steven
- *60Rr15B* borris B

Never let your card out of sight

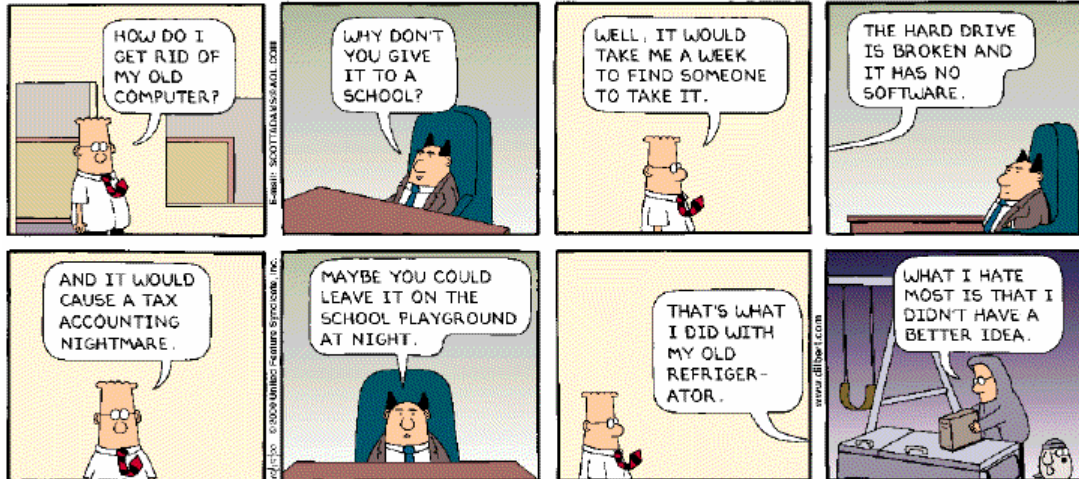
If you do, you are at risk. Dilbert did and someone cloned it and used it to buy a fur coat.



DILBERT © United Feature Syndicate, Inc.
Redistribution in whole or in part prohibited.

Destroy your old computer disks

Before disposing of your computer, remove data by using a strong "wipe" utility program. Don't just right click and "delete" to remove files and assume that a disk containing sensitive information has suddenly become secure.



Copyright © 2000 United Feature Syndicate, Inc.
Redistribution in whole or in part prohibited.

The truth is important data is always turning up on re-cycled computers.

If you haven't got a secure delete program, reboot the computer and enter bios set-up mode. In the disk menu select the low-level format option, this will re-write the disk format and take several hours. Repeat 2 times to be sure.

If you don't have the time, take the disk out and execute it with brute-force. Do the same thing to all floppy disks (what!!!) and cd/dvds

Check your statements

Each month scan your credit card, bank and phone statements, looking for unusual items. Check you credit rating by signing up to a ID theft service. There are quite a number of web sites offering this service quite cheaply. Examples are :

- Experian – Credit expert
- Garlik – Data patrol

Other tips

- Don't use a Debit Card linked to your current account to shop on-line. Use a credit card with fraud protection.
- Never enter your card details into screen that isn't protected by SSL (you known like chapter 3). Always check the SSL certificate if you are unsure.
- Shred all documents that have any personal details on them. This should include credit card offers, receipts and bills.

- When moving home, have your post redirected at the Post Office.
- When ordering a new cheque book, ask to collect it from the bank.

Stay safe – Stay you

----- end of chapter -----