



PROTECTING YOUR IDENTITY

The Scourge of the Spy Comes of Age

It used to be a piece of equipment used only by those whose job it was to protect secrets. Its effectiveness was eventually noticed by international bankers, lawyers and those who operate in the corporate world. Today, huge numbers of them are being purchased by ordinary members of the public. It is the humble paper shredder.

After a constant barrage of government warnings about credit card fraud and identity theft, the public has at last gone on the offensive. Purchases of paper shredders are outstripping sales of many domestic items at supermarkets. Yet these little machines that cost but a few pounds are also turning up on the shelves of newsagents, grocery stores and petrol stations. It seems we can't get enough of them. Don't ignore them.

For criminals, acquiring new identities and lining one's pocket at the same time from credit card fraud has become relatively easy. Creating a cloned credit card from details secured from a stolen card takes minutes. Machines and the software necessary to perform this task are available from dubious





sellers all over the world. The machines are easy to set up and can read the magnetic strip of any card and with a little know how - can bypass most security systems. It's not a subject banks like to discuss, though they are coming under increasing pressure to produce the 'totally secure credit card'. These controversial machines simply take the data and import it on a new card. An expert can produce a new card ready for use in about 10 minutes. Unfortunately the card will work on 99% of all ATMs in any country. Such machines are not strictly illegal to own or sell, but using them for such activities will result in a prison sentence. Terrorists and criminals are simply undeterred by the threat of prison for the rewards are so great.

Your credit card data appears on most receipts, gas, shopping etc. Even if some digits are not printed, criminal software can soon insert the missing numbers. Restaurants are perhaps the biggest culprits. Your details are usually printed in full, and on more than one occasion, workers have been known to sell your card information. It seems incredible that many shoppers casually discard receipts on the floor, or at the foot of ATM machines. For those who drop them in their home garbage beware - there are persons working in the underworld who are actually employed to sift through rubbish and locate your card number and bank statements.

Personal information is also a primary target - electric and gas bills, discarded photographs, holiday receipts etc. All of this is very useful to those intent on wrong-doing. The UK has a population of 60 million people. In 2001, there were 50,000 victims of identify theft. In 2005, the number of US citizens who will be exposed to such illegal activities is expected to rise above 500,000. Officially, in 2004, the British public lost £1.3bn from card fraudsters, though the figure is probably much higher.

In recent months, 'chip and pin' has been introduced at most stores. The user is invited to insert the credit card and then tap in a secret PIN number. "Much safer" proclaimed banking institutions. "Not so" say many intelligence and security experts. Criminals are using a variety of methods to observe the PIN number, from standing behind you casually in a line, to using a well-placed mirror or a second person nearby. A well-positioned covert camera will quietly go about its business for hours - clocking up the number of PIN numbers in visual form. This technique has also been used down the years to obtain the



Leaving your handbag or other personal belongings unattended on your work desk and is an open invitation to the identity thief



combination of safes. Targets are then followed and attempts are made to recover the receipt - it usually contains the credit card number and expiry date. Armed with this data, the criminal has everything he needs to make an attempt to obtain money, create a new identity etc.

Professional criminals will create accounts taking small amounts of money out of hundreds of personal accounts. Few people study statements, and even less would question a bill of \$30.00. However, criminals and terrorists are using credit card fraud to make massive profits and make purchases.

THE INTERNET STING

Using stolen credit card data to make on-line purchases is easy and can result in heartache for many small businesses. Eye Spy recently learned of an elaborate plot to acquire a huge amount of surveillance equipment that was probably intended for a criminal or terrorist gang. The operation was immaculately planned and began in Nigeria, Africa, a nation where almost 75% per cent of all the world's credit card fraud originates.

The group started by establishing various communications firms, most of them in Nigeria. They all seemed quite legitimate, directors were listed, equipment could be purchased, advertising space could be bought. There was even a telephone number. Then in April 2005, several legal surveillance stores across the world received huge orders from this firm. An order was also placed via Eye

LOSING YOUR IDENTITY

Open Doorways to Terrorism and Crime

The 9/11 Commission Report noted that impersonation is a key tool for terrorists. "Travel documents are as important as weapons. Fraud is no longer just a problem of theft. At many entry points to vulnerable facilities, including gates for boarding aircraft, sources of identification are the last opportunity to ensure that people are who they say they are."

CIA officials acknowledge that terrorism and identity theft "go hand in hand." Indeed, documentation recovered from al-Qaida training manuals, dictate that trainees to leave camp with as many as five fake personas.

Judith Collins is an identity theft expert and a professor at Michigan State University who trains law enforcement officials. She says terrorists are taught carefully in the art of subsisting off credit card fraud while living in the United States.

The Los Angeles Millennium plot terrorists, Ahmed Ressam and Mokhtar Haouari, both used credit card fraud, and even made plans to buy a petrol station and steal customer account numbers. Terrorist suspect Ali Saleh Kahlah al-Marri, is linked to 9/11 paymaster Mustafa Ahmed al-Hawsawi. When al-Marri was arrested, authorities recovered a laptop computer containing details of over 1,000 stolen credit cards. Another file had Internet bookmarks pointing to fraud and fake ID-related sites.

Some of the 9/11 hijackers used faked documents to enter the United States. The bogus papers helped them obtain drivers' licenses, which in turn assisted them in the purchase of internal flight tickets.

Former head of the US Justice Department's Computer Crime unit, Mark Rasch, said identity theft is easy and therefore makes terrorism watch lists essentially useless. "This is even more important as we start to profile terrorists," Rasch said. "With these 'red lists' we stop someone from boarding based on their ID, but it's all based on a reasonable certainty that we know who the person is."



9/11 hijackers walk straight through US airport security. Several of the terrorists used stolen identities to gain access into the United States

Spy's store for tens of thousands of dollars. We decided to examine the names of those behind the operation before we processed the credit cards. It was a thoroughly professional sting operation and we soon learned that the 'firm' was using an address that existed (street name), but the number was not real. The person behind the firm also had an array of other companies, from a 'learn to dance' agency to a car repair shop.

We decided to write to the person and notify him that his card was declined. He wrote back and sent more credit card numbers. None of the cards worked and all had different owner names - one actually belonged to a person in faraway Los Angeles. We said he could submit a bank draft to our account. It was the last we heard of him and his website's mysteriously vanished. No doubt he will be working on his next venture.



Credit card data can be used to obtain 'legal' identity papers and even passports. Keep your cards and passwords safe and apart

SAFETY AT WORK

Wherever you work, keep your personal details on your person. If you have a locker, and it is necessary to leave your wallet or bag inside, remove your credit cards, valuables and, all personal belongings. In an office environment, do not leave your personal details or bag unattended at a desk. If necessary, ask your employer for a drawer with a lock. Note any person taking an interest in what you are doing, one trick used by criminals is to browse near your desk drinking a coffee while carefully noting everything on your desk. For a few dollars, you can purchase a 'watch behind' mirror that simply attaches to your computer. This will warn you of persons taking a particular interest in what you are doing.

It's a sad fact of life, that criminals are often experts in covert surveillance. Never write your bank details or security numbers, personal codes or key words in your diary. Do not put passwords on your credit card, bank and phone accounts. Avoid using easily available information like your mother's maiden name, your birth date, the last four digits of your social security number or your phone number, or obvious choices like a series of consecutive numbers or your hometown football team. Armed with this information, the criminal can get access to your money and, probably your address.

The fewer number of credit cards you possess, the less chance of fraud. Destroy thoroughly all used cards immediately. Cutting them in pieces is not sufficient - experts can easily put the pieces back together - no matter how small they are. If your new card fails to arrive, contact your bank straight away. It is a sad fact that many cards 'go missing' in the postal system. If you are unsure - advise your bank that you



Paper shredders are available from numerous outlets and cost very little

It goes without saying, never make purchases on the Internet unless you are using a secure, reputable and, well-established company.

IDENTITY THEFT

Armed with your information, identity theft has become the fastest-growing white-collar crime in America. When persons obtain identifying information, such as a social security number, a birth date or your mother's maiden, they can usually open a new bank account, get credit etc. Terrorists are now using false details to open 'legitimate bank accounts' and can move money across the globe. Before long, the fraudster is operating in a parallel world to you. In time, however, you may receive notification of a failed repayment, and soon you will find yourself at the centre of a legal investigation, while the real culprit has moved on to his next victim.

AND FINALLY

Keep all your personal information in a safe place. When you discard receipts, copies of credit applications, insurance forms, physician statements, bank cheques and statements, expired charge cards, credit offers by mail and mailing labels from magazines, tear or use your trusted shredder.

For the cost of a fast-food meal, and becoming security aware, you can defeat those who could damage you and others forever.

The humble shredder, the scourge of many a spy, has come of age.

will pick the new card up personally - they have no right to object. Make sure you have a 24-hour telephone number on your person in the event of your card being stolen. Most opportunist thieves will use your card immediately.

The sooner you react, the less damage will be done. Take time to read the plethora of government advice that is readily available.

If you move home or office, try and advise all yours creditors and customers immediately. Use your postal service to arrange for 'inadvertent' mail to be sent to your new address until you are satisfied that everyone who needs to know where you have moved to has been informed. Unfortunately credit card and personal information often falls into the wrong hands when you move.



PROTECTING YOURSELF - A FEW TIPS

Criminals commit identity theft by stealing your personal information. This is often done by taking documents from your rubbish or by making contact with you and pretending to be from a legitimate organisation.

Identity theft can result in fraud affecting your personal financial circumstances, as well as costing government and financial services millions of pounds a year. If your identity is stolen, you may have difficulty getting loans, credit cards or a mortgage until the matter is sorted out.

The following tips will help you protect your identity and prevent criminals from committing fraud in your name:

- Your identity and personal information are valuable assets. Keep them secure.
- Regularly obtain a copy of your personal credit file from one of the three credit reference agencies to see which financial organisations have accessed your details. It is particularly helpful to check your personal credit file 2-3 months after you have moved house.
- Be extra careful if you live in a property where other people could have access to your mail. In some cases a bank or credit card company could arrange for you to collect valuable items such as new plastic cards or cheque books from a local branch.
- If you suspect your mail is being stolen check with your mail office - make sure someone has not instructed the post office to redirect your mail.

- If you move house, tell your bank, card issuer and all other organisations that you deal with immediately. Make sure to redirect any mail from your old address to your new one for at least a year.
- Keep all your plastic cards safe.
- If your plastic cards are lost or stolen, cancel them immediately. Keep a note of the emergency numbers you should call.
- When giving your card details or personal information over the phone, Internet or in a shop, make sure other people cannot hear or see your personal information.
- Never carry documents or plastic cards unnecessarily. When not in use keep them in a safe place.
- Keep your personal documents in a safe place, preferably in a lockable drawer or cabinet at home. Consider storing valuable financial documents such as share certificates with your bank.
- If your passport or driving licence has been lost or stolen contact the issuing organisation immediately.
- Don't throw away entire bills, receipts, credit-or debit-card slips, bank statements or even unwanted post in your name. Destroy unwanted documents, preferably by using a shredder.
- Check statements as soon as they arrive. If any unfamiliar transactions are listed, contact the company concerned immediately.
- Keep your passwords and PINs safe
- Never give personal or account details to anyone who contacts you unexpectedly. Be suspicious even if they claim to be from your bank or the police. Ask for their phone number, check it is genuine and, if so, call them back. Be aware that a bank will never ask for your PIN or for a whole security number or password. Keep them secure.
- Don't use the same password for more than one account and never use banking passwords for any other websites. Using different passwords increases security and makes it less likely that someone could access any other accounts.
- Keep your passwords safe and never record or store them in a manner which leaves them open to theft, such as in your purse or wallet.
- If you receive a suspicious e-mail purporting to be from a bona fide institution which requests personal details don't reply and simply delete.