



David Hill

Secure IT

Identity theft and fraud can be an inconvenient and costly business for individuals and companies alike. Many are unclear as to what steps need to be taken to avoid becoming a victim. David Hill outlines a basic plan of action for security professionals and their members of staff.

Identity theft: don't be the next victim!

IN THE UK, IDENTITY THEFT IS AN increasingly common crime, costing the country an estimated £1.7 billion in the last year alone. In this current 'fraudster' environment, the confidentiality of information is ever more vital. Businesses must be fully aware of the risks, and continually educate employees on the protection of data.

Criminals rely on being able to take advantage of peoples' trustworthy – and often careless – nature to access sensitive information about individuals, Government departments and private sector organisations. This is used for a range of criminal activities, from directly accessing accounts through to creating false identities and applying for financing and official documents.

Sensitive business information can also be sold to competitors, or used to defraud customers and/or the business as a whole.

Though the issue of identity theft has been much publicised, increased public understanding has not yet resulted in a drop in the incidence of this kind of crime. While many individuals are more and more aware of the risks, they are either unclear on what to do to avoid becoming a victim of identity theft and fraud, or they are simply unwilling to take the necessary steps.

It's absolutely essential that we start taking this problem seriously and make the simple changes that can help us avoid the inconvenience and cost caused by identity theft and fraud.

Shred... but don't phish

Never give out your personal details unnecessarily. Some people have become victims of identity theft merely because they have offered these details – such as their date of birth and home address – to fraudsters. Fraudsters call, claiming to be from a recognised financial institution, and then start asking questions. Recognised financial institutions will never ask for your personal information – they already have the necessary 'intelligence' you've provided on file.

Ensure that you shred your personal documents, such as bank statements. Fraudsters are increasingly resorting to 'bin raiding' whereby they will sort through your rubbish in search of documentation. The only effective way to ensure that your documents are disposed of properly is to destroy them in a cross-tooth shredder or, if you have a fireplace, burn them.

Do not succumb to phishing e-mails. A phishing e-mail is one that pretends to be from a recognised institution, like eBay or Citibank, and asks you to input your account data (such as login details). These scams are often supported by fake, spoof web sites and victims are tricked into thinking they are logging on to a real web site. The key to these e-mails is that the fraudsters request the release of a combination of personal information, such as PIN numbers, date of birth and home address on the premise that the recognised institution in question has misplaced those details. Bear in mind that recognised institutions will never ask for your personal details via e-mail. They already have this information to hand.

Take proactive steps to ensure that the information on both your laptop and mobile is inaccessible in the event that either is stolen. Use a password protection measure to make certain that the person in possession of your laptop is unable to log on.

When leaving your laptop unattended either in your home or at your place of employment, secure it to an immovable unit with a cable lock. If possible, do not keep sensitive information – such as bank account numbers and PIN numbers – on your laptop.

Download up-to-date software

Keep your mobile phone locked and, ideally, off when not in use. Ensure that your computer is adequately protected. Download up-to-date

anti-virus software on a regular basis and ensure that you have adequate firewalls in place. This will mitigate the risk of fraudsters picking up your personal information while you are banking or shopping online.

When travelling, ensure that your passport is always in a safe place. If possible, leave the original in a hotel safe and carry photocopies of the original. If your passport is stolen, contact the Passport Office immediately.

If you should lose your wallet, cancel your cards immediately. Should this situation arise, ensure that you report all lost cards to the relevant authorities. They will then inform you of the appropriate action to take. Although the chances of an identity fraudster actually coming across your details because of this (fraudsters tend to proactively attempt to compromise your identity), it's best to take all necessary precautions to ensure that you do not lose either your identity or your finances.

Monitor your accounts. Keep a close eye on your banking accounts for any unauthorised direct debits being set up without your permission. Fraudsters have been known to start skimming slowly off the top of victims' bank accounts to see if they notice. Once it's clear they do not, increasingly large sums of money are withdrawn. Check your statements carefully each month and sign up with a credit reference agency – such as Equifax – to monitor your credit rating.

Be vigilant when withdrawing cash from an ATM. Do not accept help from strangers, no matter how friendly they may seem. If your card is swallowed by the ATM under suspicious circumstances, ensure that you report the matter to your bank right away.

Safeguard your PINs

It may sound blindingly obvious but always be vigilant with your passwords and PIN numbers. Do not give out your PIN numbers to anyone. Ensure your passwords are an alpha-numeric unique combination, and that they are different for each of your various accounts.

Commit your PIN numbers to memory. Never keep a written copy of your PIN number with your credit and debit cards. Cut and paste your password from a Word document into your log-in field when working online as this will render keystroke software useless.

By following these straightforward steps, individuals and businesses alike can dramatically lower the risk of becoming victims of identity theft and fraud. Simple steps that could save you a whole lot of trouble. ■

■ David Hill is senior security consultant at red24 (www.red24.info)

“While many individuals are more and more aware of the risks, they are either unclear on what to do to avoid becoming a victim of identity theft and fraud, or they are simply unwilling to take the necessary steps”