



Reduce your Risk of Credit Card & Identity Fraud

This is the ITSecurityExpert's guide for reducing personal risk of **Credit Card Fraud** and **Identity Theft**.

20 Tips for Reducing the Risk

1. Invest in a decent shredder, avoid cheap shredders they are a false economy, they often don't last long anyway, and can make shredding a real chore. Try to get into the habit of regularly shredding receipts, statements or anything else with financial and personal information. Value the importance of documents, for instance a couple of utility bills can be enough to steal your identity, so shred them if you don't need them, protect them if you do.

Do not ignore all the health safety aspects of owning a shredder, especially if there are children in the house. Read the instructions



£50 to £75 can buy you a quality "crosscut" shredder (above right) which shreds 12 pages at a time, even with staples, and can also shred DVD/CD and credit cards.

2. Never ever disclosure your PIN number, login details or passwords. Often fraudsters will "confidence trick" by appealing to either greed or fear. For example if you are told you have won a competition or entry into a free cash draw, but you have never entered the competition, I 99% guarantee it is either a fraud scam or an attempt to collect your personal details for marketing, just remember there is no such thing as a free lunch. Fraudsters will use fear to bypass your normal cautious thinking, by impersonating organisations like your bank or your favourite online auction site, stating they have detected a security breach with your online account, and that you must validate your details.

3. Never ever write down passwords, login details or especially Chip & Pin number.

4. Never send card details or any bank details by Email, even if a hotel or online shop requests your card details by Email. My golden rule with Email security is, if you are not happy to write the Email contents on the back of postcard and post it, you shouldn't be writing within an Email, as Email is not a secure medium. Also when reading your Email, the senders Email address and Name is absolutely no guarantee the Email was sent from that person or organisation, and of course never accept Email attachments, or click on links within Emails you aren't sure of or were expecting.



5. Never let your debit/credit cards or your card details out of your sight when making a transaction in the real world. Unfortunately low paid shop staff are some of the worst culprits when it comes to card fraud, either collecting card details and selling them on, or committing fraud directly themselves, it can only take seconds for them to steal the info from your card when out of view.



Shield as you type in your pin number

6. When using a Chip and Pin devices or cash machines, use your free hand to shield the number pad as you type in your PIN. This will provide protection against bad guys who “shoulder surf” and hidden cameras, which can be impossible to spot.

7. Never use a cash machine you aren't sure of, if it looks a bit suspicious and you have never used it before, go with your instincts.

8. If you can, avoid divulging your card details by telephone. You don't know who might be listening nor can you see the person collecting details, and what they might do with them.

9. With online banking, always type in your bank website address directly in the address bar of your web browser. Never click on web links, especially those sent in Emails.

10. If you get a telephone call explaining you have been a victim of fraud by your bank, which could be totally legitimate, don't discuss any details, hang up and phone your bank using the number on the back of your card. Fraudsters are increasing using internet based phone calls to ensnare victims, usually targeting victims specifically, for them it is cheap and hard to trace.

11. At all times, make sure your computer has up-to-date anti-virus software, up-to-date Microsoft Windows Patches, Anti-Spyware and a Firewall installed and Enabled.

12. When shopping online, make sure the webpage is encrypted before entering any personal and credit card details. Look for a locked golden padlock and “https” at the start of the web site address. You probably wouldn't give your credit card details to a street trader right? Well consider the same approach when shopping online. If a website looks dodgy and you have never heard of the business, the offer is too good to be true, you probably should go with your instincts, as you would in the real world.

13. Always check through your bank and card statements, and chase up any anomaly you find, even the smallest unexplained transaction could be a sign of identity theft or account compromise.



14. When filling out forms or being asked for personal information verbally, never be afraid to question what you are supplying, as it is all too easy to go into autopilot. Let's say if someone knocks on your front door promoting a new local car wash, and gives you a discount voucher and then proceeds to ask for your name, Email and phone number. Ask yourself why that information is being collected and question the promoter about what the car wash company will do with it. Don't be afraid to question organisations as well, about how they are going to protect your personal information, read up on their privacy policies before parting with your personal information, know what you letting yourself in for.

15. Always keep your guard up, this is not as easy as it seems. We are all bombarded with requests for our personal information on a daily basis, whether via a street survey, or a small opt in/out check box within the small print within forms, always try to avoid giving up your personal information unnecessarily, often the people collecting it will sell it on to marketing firms for a profit or even worst.

16. Keep track of your bills, if every month you get a credit card statement, and one doesn't turn up, make a point of chasing it up. Also when you receive a new cheque book, check all the cheques are present, one cheque scam often committed by fraudsters, is to intercept cheque books in the mail, open it and steal a couple of cheques from near the back of the book and then cash them, before resealing and placing by in the post. It is often far too late before the victim discovers the missing cheques.

17. If you don't need it, don't carry it. Avoid carrying all your identification information and cards in your wallet, on your person, and within your bag. At home, look after and put away all your key identification documents like passports in a safe.

18. If you lose or have stolen important identifying documents like a passports, driver's license, birth certificate, be extra vigilant and ensure you do everything possible with the necessary authorities to reduce the risk of their misuse.

19. Be careful what you post up about yourself on the Internet, particularly on social networking sites, as often fraudsters who commit identity theft will use any personal information they can find out about you to aid them. Your date of birth, the schools you attended, where you work, your mother's maiden name, your favourite football club and even your hobbies are typical types of personal information that can be used against you. The biggest security flaw with any social network sites is with the "friends" who you allow and trust access to your personal space and information. It is very difficult to know for sure if a friend from your past is really that. Social Networking wise, try to ensure your private information stays private by selection the appropriate online profile options, and you don't circumnavigate that by allowing friends who are really strangers, into your online circle of trust. Also be careful using messenger services like Windows Live/MSN Message, never ever supply personal or card details even if it looks like a friend or relative is asking.

20. If you feel particularly concerned that you might be a victim of identity theft, arrange a credit check with credit reference agencies on yourself, and chase up anything suspicious found to the source.



FAQs

Q. What is Identity Theft?

A. Simply put, it is when a someone assumes your identity and racks up credit\loans in your name with no intent of paying it, and/or commits to other fraudulent and criminal activity in your name.

Q. Why Identity Theft bad?

A. Being a victim usually means your credit rating is destroyed, which can be very difficult to put right. Also in most cases people don't find out they are a victim until for months or even years. I have heard of one couple losing out on purchasing their dream house for instance, due to being rejected for a several mortgages, as unknown to them at the time, one of them were a victim of identity theft. Other side effects result in receipt of repayment demands for credit you have never taken and threats of bailiffs and court action, which can all be extremely distressing and a difficult process to correct.

Q. Who committing Identity Theft & Credit Card Theft?

A. Well it not just the usual stereotypical criminal elements that are involved, it can anyone, and it usually is. Prime candidates are employees in low paid jobs ensured with accepting card payments, have been known to harvest credit card details, and then sell them up to criminal gangs. Even call centres have been targeted and infiltrated by criminal organisation to gain access into this lucrative trade. I have even heard of cases where family members have assumed identifies of other family members.

Q. I'm a victim of Credit Card Theft?

A. Contact your card provider immediately; usually it can be a fairly simple process, as long as you haven't done anything silly like write your pin number down. Credit Card companies are usually pretty good and proactive in spotting fraud patterns and the majority will reimbursed you fully if you aren't to blame.

Q. What are the tell-tale signs that I'm might be a victim of Identity Theft?

A. There are several signs to look out for:

- You are unexpectedly rejected with loan or credit card applications, even though you have a good credit history
- If you receive debt collecting mail from companies and solicitors for debts you know nothing about
- Missing post, expected bank and credit card statements, and especially replacement credit cards and cheque books do not arrive
- You receive bank and credit card statements that you haven't setup or hire purchase agreements or mobile phone contracts you know nothing about
- You receive bills, invoices or receipts addressed to you for goods or services you haven't used or asked for.



ITSecurityExpert.co.uk

Get Secure, Be Secure & Stay Secure

Q. What if I'm a victim of Identity Theft?

A. Well there are many steps to be take, but I recommend the following three steps to start the ball rolling.

Absolutely the first step you should do is report it to the police, it is fraud which is a crime, even if it seems unlikely the police can resolve it or if the police officer you deal with doesn't take your report too seriously, make sure it is recorded and obtain a crime reference number, and note that number.

The next step is to contact (all) the organisations involved with the identity fraud, making sure you speak with right people within each organisation, identity theft isn't uncommon, so you should find most organisations can help you with putting things straight.

The third step is to contact credit reference agencies, and start to put things right with them, there are third party companies that can help in this regard.



www.itsecurityexpert.co.uk

Written by David Whitelegg

Document Disclaimer

While every reasonable precaution has been taken in the preparation of this document, neither the author nor ITSecurityExpert Limited assumes responsibility for errors or omissions, or for damages resulting from the use of the information contained herein.

The information contained in this document is believed to be accurate. However, no guarantee is provided. Use this information at your own risk.

www.itsecurityexpert.co.uk