Advice on Identity Fraud

Identity Fraud

Identity Fraud is often quoted as the fastest growing crime in Britain. Identity Fraud involves the misuse of an individual’s personal details in order to commit crime. Your personal details are very valuable to the criminal who can use these details to commit crime or even sell them on to other criminals.
Victims of identity fraud often suffer a great deal of stress and cost in trying to clear matters up after the fraudulent use of their personal information. Many never establish exactly how their details were obtained.

Protecting your address.

If you start to receive post from someone you don't know, find out why.
Register to vote at your current address (Lenders use the electoral roll to check who is registered as living at a particular address)
When registering to vote, tick the box to opt out of the "Edited" register to prevent unsolicited marketing mail. (This does not affect credit checks)
Sign up with the mail preference service to prevent marketing letters. (M.P.S. is a free service enabling consumers to have their names and addresses removed from mailing lists:- Telephone 0207 2913300 or www.mpsonline.org.uk
Protect mail left in communal areas of residential properties.
Re-direct your mail when moving home.
Do not leave documents containing personal information in view, for example on window sills or where the general public can view them or has access to the location. (Communal areas)

Protecting your Bank Account

Be extremely wary of unsolicited phone calls, letters or emails from your bank, or other financial institutions, asking you to confirm your personal details, passwords, pin numbers and security numbers. (A Bank will never ask you to reveal your pin number. It’s yours and yours only.)
Regularly check your accounts and chase up any statements that are not delivered and expected.
Dispose of anything containing your personal or banking details by using a cross cut shredder, tearing them up into tiny pieces or incinerating them.
Always sign up to American Express SafeKey, Mastercard SecureCode OR Verified by Visa when you receive your cards, even if you don't intend to use your cards online. This helps to protect you if your card or details are stolen or lost.

If you think someone is misusing your bank account details then report it to your bank.

Protecting Your Phone

Never reply to unsolicited Texts, e.g. Texts referring to accident claims, even to try and get them stopped. Simply delete them.
Sign up to the Telephone Preference Service to prevent marketing phone calls. (T.P.S. is a free service. It is the official Opt out register on which you can record your preference not to receive unsolicited sales or marketing calls. To register 0800 398893 or www.tpsonline.org.uk
If using a "smart" phone install anti-virus software on it.

Protecting Your Computer

Keep your computer security programs such as antivirus and firewall, up to date. Also make sure your web browser and operating system are the latest version. If unsure how to do this contact a computer specialist.
Be wary of opening links on unsolicited emails you receive. They may contain viruses or other programs that may harm your computer.
Know how to verify secure web sites if making financial transactions. You can do this by looking at the address line. Normally it will start with http but when you log into a secure site this will change to https. For example http://www.mybank.com is the address of mybank, but if you want to go to the transaction page you log in and the address bar will change to something like https://mybank/login.com The address bar may also change colour. A padlock will appear in either the bottom left or bottom right corner of your browser bar, not on the website.
If you have received an email claiming to be from your bank, asking that you contact them, think about whether or not it’s genuine. DO NOT click on links in the email, open another window in your browser and visit your banks website using your normal method.
Check online banking security options your bank provides, some offer free anti-virus and browser security software.

Never reveal pin numbers
Never click on links on emails (go to the actual website)
Never open attachments unless it’s from someone you can trust.
Contact them first if you’re unsure it’s genuine.

Your Personal Information is Valuable, Take Action To Protect It.