



IDENTITY FRAUD

Updated November 2006

Based on an original
development by EASTBOURNE
CAB funded by EDF ENERGY



Identity Fraud is when someone uses your personal information to obtain credit or buy things in your name.

It is the fastest growing crime in the UK. It is estimated criminals obtain £1.4 billion a year this way.

You may not realise it is happening until some time has passed. You may find you are refused credit, you get bills for things you have not bought or are contacted by debt collectors for debts which aren't yours.

The effects of Identity Fraud can be very difficult to sort out.

Protecting your personal information has become increasingly important.

Once a fraudster has your personal details they can

- open new bank accounts
- spend money and leave you with a bill
- obtain false documents such as passports or birth certificates
- commit benefit fraud

Protect yourself against Identity Fraud

Dispose of anything containing your personal details carefully.

A letter addressed to you containing your name and address or further details like account numbers could be taken from your rubbish and used by a fraudster.

Always make sure these letters are destroyed carefully.

Rip them into pieces or use a shredder before throwing them away.

Important documents that you want to keep should be locked away safely at home or kept at a bank or solicitor's office.

Lost or Stolen Cards

If you lose a debit or credit card or you think it may have been stolen contact your card provider immediately. It is worth making a note of the emergency number for reporting lost and stolen cards. It should appear on the back of your statements.

When you report a card as lost or stolen the bank will immediately put a block on the card which will prevent anyone from using it.

You will be sent a new card within a few days and a new pin number if required. The card and pin number will usually be sent out separately.

Once you have received the pin number you should memorize it and destroy the letter it came on.

Credit and debit cards have an expiry date, after which they cannot be used. Before this date the bank or lender will send you a new replacement card.

You should dispose of the expired card carefully to make sure the details it contains cannot be used by anyone else.

Cut the card into pieces and throw it away.

Lost or stolen documents

Driving Licenses and Passports can be used to open bank accounts or obtain credit. They would have to be accepted as proof of identity by a bank or other lender. Both have a photograph of the holder which should make it more difficult for someone else to use them.

If you think your driving license has been lost or stolen you should report it to the police as soon as possible. You can obtain a duplicate license from the DVLA using form D1 which is available from the Post Office.

If you think your passport has been lost or stolen while you are in the UK you should report this to the police. You can obtain a replacement passport using form LS01 which is available from the police station and post offices.

“Phishing”

Internet banking is increasingly popular but it offers new opportunities for criminals to get their hands on your money.

A common method is known as “phishing”.

You receive an email which appears to be from your bank and asks for you to update your account details. It may include the bank’s logo and have a return email address which looks genuine.

NEVER RESPOND TO EMAIL REQUESTS FOR BANK DETAILS

If you respond to the email and give your details the fraudster will be able to have full access to your bank account.

Your bank will never ask you for your personal details this way.

If in doubt contact your bank and tell them what has happened.

Here is an Example of a scam email

Dear Anybank PLC online customer

For security purposes your account requires verification.

To verify your account information we are asking you to confirm your account details and personal information.

If you do not confirm these details within 14 days your account will be suspended.

Please click on the link below to access Anybank PLC secure page and verify your account details.

Thank you.

<https://anybankplc.co.uk/verify>

Anybank PLC is authorised and regulated by the Financial Services Authority

Although the message appears to be official, it is not.

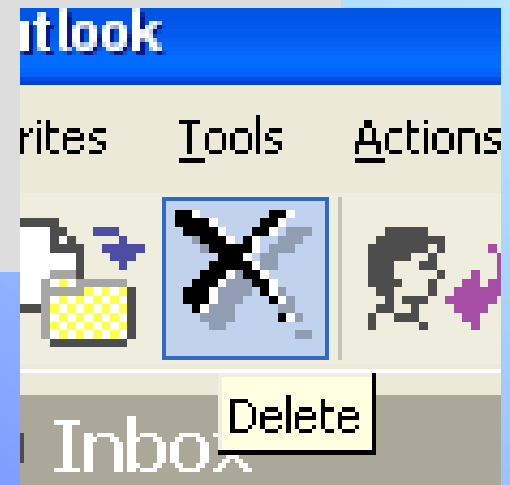
The email has been written and sent to you by a criminal, not from your bank. The location of the criminal is unknown. It could be from anywhere in the world.

Notice how they make the message sound as if it is to protect the security of your account. They also say your account will be suspended in 14 days to worry you. In fact, if you do not respond to the instructions nothing will happen after 14 days.

The last sentence may be true but it has nothing to do with the sender of the email.

The best thing to do with messages of this kind is

DELETE.



The same applies to phone calls asking for personal details such as account numbers or pin numbers.

NEVER GIVE OUT YOUR PIN NUMBER OVER THE PHONE

Your bank will never ask you for your personal details this way.

If you need to give details over the phone for example ordering goods with a credit card, make sure you know who you are speaking to.

Make sure other people cannot overhear you if you are giving your card details over the phone.

There are many variations on email scams which attempt to lure you into giving away personal information, often by telling you you have won a prize. Many of these originate overseas or at least the email says that.

Similar scams work using letters telling you you have won a prize and in order to collect the money you must give them your bank account details.

If an offer looks too good to be true – it usually is!

NEVER GIVE OUT YOUR PERSONAL INFORMATION TO A REQUEST MADE IN THIS WAY.

If you receive any letters or emails of this type, delete them or throw them away.

Protect your computer

Install good quality

- anti-virus software
- spyware removal software
- spam filter – your email provider may offer this service
- firewall – included as a part of some operating systems

and keep them up-to-date. Run regular scans.

Keep your operating system up to date and apply any security patches.

Use the most up to date version of Internet Browser

- Don't store your password or pin number on your computer.
- Don't write down your passwords and leave them where they can be found.
- Do not save passwords on computers that are used by other people.
- Don't use passwords which can be easily guessed such as your middle name, date of birth etc.
- Never tell anyone else your password or pin number.
- Change your passwords regularly.

Find out if you have been a victim of fraud

It is a good idea to check your bank and credit card statements when they arrive. If you notice any amounts which you do not remember or believe you have not paid for you should contact your bank or lender immediately.

You can also obtain a copy of your credit record which will show all the accounts you have open. If you find an account you did not open you may be a victim of fraud

You can get a copy of your personal credit file for £2 from one of the three credit reference agencies.

Callcredit PLC

Consumer Services Team
PO Box 491
Leeds
LS3 1WZ
Helpline: 0870 060 1414
www.callcredit.plc.uk

Equifax PLC

Credit File Advice Centre
PO Box 1140
Bradford
BD1 5US
Tel: 08705 143700
www.equifax.co.uk

Experian Ltd

Consumer Help Service
PO Box 8000
NOTTINGHAM
NG1 5GX
Tel: 0870 241 6212
www.experian.co.uk

Possible signs of Identity Fraud

- When you apply for credit you are turned down despite the fact that you have a good credit history and no record of defaulting
- Your credit file shows entries which you do not recognise
- You are contacted by a debt collection agency for an amount which you do not remember borrowing
- You do not receive bank or credit card statements which you are expecting
- Your passport or driving license have been lost or stolen
- When you apply for benefits you are told you are already receiving them when you are not

What to do if you have been affected by Identity Fraud

- Get a copy of your credit file from the credit reference agencies. If you find entries from finance companies you do not normally deal with contact them straight away by phone followed by a letter.
- Report it to your local police and request a crime number.
- Report any lost or stolen documents
- Send letters by recorded delivery and keep a record of the time taken in sorting out the problem.
- Inform [Royal Mail](#) if you think your mail has been stolen or that a mail redirection has been fraudulently set up on your address
- If you have reason to believe your address is being used by someone to commit fraud you may wish to register with CIFAS Protective Registration Service. This gives some protection against fraud and helps prevent it from continuing. For further information visit www.cifas.org.uk

Further information:

CIFAS www.cifas.org.uk

Home Office www.identity-theft.org.uk



IDENTITY FRAUD

END