



**POLICE
SCOTLAND**

Keeping people safe

Victims of Fraud

What is Fraud

Fraud is a crime in which some kind of deception is used for personal gain. Fraud is sometimes also referred to by other names such as a scam or con.

Advice for Victims of Fraud

If your bank or credit card accounts have been compromised contact your bank and tell them you suspect you have been the victim of a fraud.

If you receive correspondence from companies about applications or accounts that you do not recognise, contact the relevant companies immediately and advise them.

Report the fraud to Police Scotland on 101.

Keep a note of any telephone numbers, emails or other correspondence you have had with the fraudster.



Consider contacting a credit reference agency to review your credit report. If you notice any unauthorised activity contact the organisations involved, as soon as possible.

If you have been a victim of fraud be aware you details might be sold on to other fraudsters who might make contact with you in an attempt to make you part with more money. This is most common in the case of victims of share scams. Fraudsters often call up the victim of such a scam advising they can get their money back for a fee.



Cold Calls

There are numerous cold call scams. Some of the most common types are:

1. A call is received from a fraudster purporting to be calling from a government body such as HMRC advising that a fine must be paid immediately or there will be court action.
2. The fraudster promises a large PPI refund but first taxes or fees have to be paid. No PPI refund is ever received.
3. The fraudster advises they are calling from Microsoft, BT or Talk Talk and that there are problems with the victim's computer or broadband. The caller may know personal details and ask to be allowed access to the computer. The fraudster may instruct the victim to open their online banking or make a payment by a money transfer service. No reputable company will make contact with you in this way or instruct payment to be made in this manner.
4. The fraudster pretends to be calling from the victim's bank advising of suspicious activity and thereafter induces the victim to hang up the telephone and call the number on the back of their bank card. In these cases the fraudster stays on the line pretending to be a representative of the bank, then instructs the victim to transfer money into a 'safe account'.

Your bank will never ask you to transfer money into another account. If you receive a phone call, apparently from your bank, under the above circumstances, call into your local branch or phone your bank using a different telephone. Alternatively wait until you have heard a dialling tone before phoning your bank.

Consider contacting your local Trading Standards office who will be able to provide advice on approved call blocking systems.

Fraudsters want payment in a manner that is difficult to trace such as money transfers or gift vouchers. No reputable business or government body will ever instruct you to pay fees or fines in this manner. If in doubt, request that the caller puts the instruction in writing. If a letter is received and you are still suspicious, call Police Scotland on 101.

Fraudsters change their methods frequently. If you are at all suspicious note as much information as you can and ask for a letter to be sent to you. If you receive a letter and are still suspicious call Police Scotland on 101.

Buying and Selling Online

A high proportion of online fraud is perpetrated via online classified services such as Gumtree and on auction sites such as Ebay. The easiest way to stay safe when buying and selling on these sites is to buy and sell locally. If you are buying, go and see the item at the seller's address along with a friend or family member. If you are selling an item, then only accept cash or other secure payment and do not post the item to a buyer until the money has been received.

Sometimes the fraudster sends an email to the seller which appears to be from an online payment site such as Paypal. The email advises that payment has been received and it is safe to post the item. Always verify the email address and check directly with the payment site.

Be especially careful when purchasing expensive items such as vehicles and machinery online, and when buying concert tickets.

If you have been the victim of a scam, contact the selling site as well as the police.



Renting Property

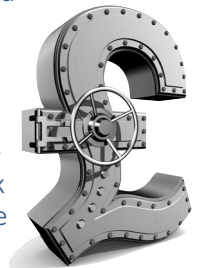
If you are looking for a property to let, never part with money before viewing the property and verifying the landlord's details.



The Landlord Registry Service (www.landlordregistrationscotland.gov.uk) provides details of most private landlords.

Loans

If you are applying for a loan via a loan brokerage site or through a payday lender, please be advised that legitimate companies will not ask for you to pay advance fees into a personal bank account by money transfer or gift voucher.



Beware of illegal money lenders and report any suspicions to the Police or confidentially to www.stoploansharks.org.uk

Lottery and Inheritance Scams

There are numerous scams relating to non-existent lottery wins and unexpected inheritances.

Lottery scams are where the fraudsters send out letters to members of the public with promises of large lottery wins. The victim is advised not to mention the win to anyone. The victim is encouraged to phone or fax the fraudster and is thereafter instructed to pay various 'fees' to release the win.

The inheritance scam generally relates to someone with the same name as the victim who has died in a foreign country and has left a large inheritance but with no beneficiary. The fraudster tries to get the addressee to make contact with a view to moving the non-existent money. Of course demands for banking details or fees follow.

Other useful advice

If you have been asked by a vendor, landlord, loan company or someone you have met on a dating site, to send money by a money transfer service (eg. bank transfer, iTunes voucher, Western Union or Moneygram), please read the advice provided by these companies and online advertising sites (eg. Gumtree, Ebay) before carrying out the transfer.

Fraudsters often target the vulnerable and the elderly. On occasion a victim can get caught up in a long term scam where they are induced to receive and send money on behalf of the fraudster for an apparently legitimate reason. This can cause considerable stress to the victim who may also be receiving a large volume of junk mail. Contact Police Scotland on 101 if you feel you or a relative have been caught up in such a scam.

A comprehensive list of the main fraud types can be accessed on the Police Scotland website at: www.scotland.police.uk/keep-safe/advice-for-victims-of-crime/fraud/main-electronic-fraud-types.



Remember

- Ensure you have adequate anti-virus protection on your computer and keep software up to date.
- Be wary of clicking on links or web pages especially links in unsolicited emails.
- Never give out login details in an email or over the telephone, no matter how genuine you think the request is.
- Be wary of the information you are giving out on social networking sites (contact details, date of birth etc).
- Do not include your birth date or address in your email address.
- When you are finished with personal or financial documents, shred them before you throw them out.
- Be wary of cold calls. If in doubt just hang up, and never give out personal or financial information if you are unsure who you are dealing with.
- No reputable company will instruct you to make payment by money transfer or by gift voucher.
- Call Police Scotland on 101 if you are unsure or require advice.

Useful links

www.cifas.org.uk - for advice on protecting your identity

www.getsafeonline.org

www.fca.org.uk

www.equifax.co.uk - for credit checks

www.experian.co.uk - for credit checks

www.mpsonline.org.uk - to remove your address from mass marketing mailing lists

www.tpsonline.org.uk - to remove your telephone number from mass marketing call lists

www.royalmail.com - to report nuisance mail

