Fraud

Your guide to protecting yourself from fraud

FRAUD ISN'T JUST A SCAM
IT'S A CRIME

Kent Police

Kent Police is committed to protecting people from career criminals and fraudsters.

This booklet has been designed to give you advice on how to protect yourself and your friends and family. It contains the most common methods used by fraudsters along with top tips on how to avoid becoming a victim.

Please pass on this information to anyone you think may find it useful.

Protecting yourself, your family and friends

- Never give personal details (name, address, bank details, email or phone number) to anyone without checking they are genuine. The police and financial organisations will **never** ask for account details over the phone.
- Always check the identification of anyone you are considering buying a service or goods from.
- If someone offers you goods or a service that seems too good to be true, it could be a scam. Don't feel pressured into taking up an offer before you've checked the company or individual is genuine. If you have concerns or are put under a lot of pressure, just say no.
- Shred documents containing personal information before throwing them away and keep personal documents in a safe and secure place at home.
- Check email addresses. Fraudsters sometimes use false accounts to con people. For example, 'info@ebayz.com'. The real address would be 'info@ebay.com'.
- Make sure your computer, tablet or smartphone has anti-virus and anti-spyware software. If you are unsure how to do this, visit **www.getsafeonline.org**

When to take action and contact Action Fraud on **0300 123 2040**

- If you receive a bill for something you haven't bought.
- If you think you may have responded to a fraudster without realising it.
- If you have given someone your bank details and you are worried they may not be genuine.

Action Fraud will give you advice on what to do next.

If you have concerns that elderly or vulnerable neighbours, relatives or family have been targeted, talk to them and check they are OK.

If you need more advice, contact Action Fraud or visit their website **www.actionfraud.police.uk**

ActionFraud

Report Fraud & Internet Crime

actionfraud.police.uk

FRAUD ISN'T JUST A SCAM IT'S A CRIME

Types of fraud

Identity fraud

Identity fraud is when someone uses your name or details, usually for financial gain.

Fraudsters may try and get your personal details through a variety of methods:

- **In person** – They may knock at your door and ask for personal information. They may pretend they are selling something, providing a service or carrying out a survey. Sometimes they will pretend to be from a reputable organisation.
  Remember you can just say no and close the door.
- **By phone** – A fraudulent call centre may try and get your personal information. Sometimes they will send a text to your phone, pretending to be from your bank, and ask for your account details.
  Remember you can just say no and hang up.
- **By email or letter** – A fraudster sends correspondence pretending they are from a legitimate organisation. They may use the legitimate organisation's logo and link to a website that is set up to look like the real thing. They will try and get you to enter a website using your password or send your details by email.
  'Spam' email (contact that you haven't requested) may also be sent to try and get access to your details electronically.
  Remember you can just ignore the email/letter.

If you are suspicious of any contact made by these methods:

- Don't reveal any personal details
- Don't enter any websites using your normal password
- Delete emails you are suspicious of
- Don't click on any hyperlinks
- Report it to Action Fraud

Advance fee fraud

This is when fraudsters ask you to make upfront payments for goods or services or an opportunity to make money.

Some common examples:

- **Letter fraud** – victims are asked to allow the transfer of money from another country to your account. They say they will give you a percentage of the money in return for doing this. They may pressure you to meet up. They will ask for your account details.
  Never reply to letters or emails from these types of fraudsters.
- **Lottery fraud** – fraudsters contact you to say you have won a large sum of money through a lottery, sweepstake or prize draw. If you respond you may be asked to: provide personal information (that could be used to steal your identity), pay upfront fees (before you can receive the non-existent winnings) or be asked for your bank details (so they can empty your account).
  Never respond to this type unsolicited contact. Think about any competitions or lotteries that you have taken part in and contact the organisation directly.
- **Dating fraud** – if you use dating sites don't start giving people money. Be careful with people who want to make contact with you outside of the dating website. Don't give them personal information such as your bank details and don't send compromising pictures that they could use against you.

Types of fraud

- **Courier fraud** – fraudsters call you by phone pretending to be from your bank, or the police, and will tell you your account has been accessed fraudulently and they need your account details and bank cards. They will tell you to call your bank straightaway to check the request for bank cards/ PINs is genuine. They keep the line open so you think you are calling your bank, but in fact you are simply talking to another fraudster. They then tell you to hand over your bank cards and PINs to a courier/delivery service that will call at your house to pick them up.

  If you receive a call like this, call your bank from another phone. If you don't have another phone, ask a family member or neighbour for help.

But remember

The police or bank will:

- never ask you for cash, valuables or your PIN
- never send a courier to your home
- never collect your bank card
- you can just say no and hang up

If you receive a call like this, call Action Fraud for help.

Rogue traders

Some people who try and sell you goods or services by knocking on your door are genuine. However, some are fraudsters who will overcharge or take money and never deliver the goods or provide the services.

There are laws around door-to-door selling and even if a rogue trader gives you a 'cooling off' period, they will not honour it. Sometimes criminals will pose as salespeople to gain access to your home to steal property or assess your home for a future burglary.

Top tips:

- Always check identification before letting someone you don't know into your home.
- If you are interested in a product, ask the seller to leave their contact details so you can call them later. A genuine salesperson will accept this.
- Don't sign up to something on the spot. Shop around and get some alternative quotes.
- Never reveal personal information.
- If in doubt, ask the person to leave.
- Always ask for references if the goods or services cost a lot of money.
- Always get any agreement in writing.
- Don't have any work done or goods delivered in the cooling off period. You may have to pay even if you change your mind.
- Never pay for work before it has been completed, and only then if you are happy with it.

Report rogue traders to Trading Standards

- Contact the Citizens Advice consumer service on **03454 040506**, Monday to Friday, 9am to 5pm
- Visit **www.kent.gov.uk/tradingstandards**
- Text '**Rogue**', space then the details to **07860 00 80 25**

Types of fraud

Boiler room/share sale fraud

This type of fraud involves bogus 'stockbrokers', usually from overseas, pressurising you into buying shares in companies that promise high returns. The bogus stockbrokers always sound very professional and convincing and will try and rush you into a decision. They may also produce false share certificates and have fake websites.

Top tips:

- If you have concerns contact the Financial Conduct Authority on **0800 111 6768**.
- If the returns on an investment sound too good to be true, then it could be a fraud or come with a very high risk.
- If you are suspicious or have concerns, don't invest.
- Remember that if the fraud is being operated from abroad and not covered by UK compensation schemes, you are unlikely to recover any money.

Pyramid scheme

Fraudulent pyramid schemes involve enrolling other people into a business that offers a non-existent or worthless product. You have to pay a fee to enter the scheme and recruit others – there is usually no investment and people end up losing money. Fraudsters will pressure you to join.

Top tips:

- Ask questions and be suspicious if the person selling the scheme dodges questions.
- If you have concerns, contact the Financial Conduct Authority on **0800 111 6768**.
- Remember, there is no such thing as a 'guaranteed risk-free investment' – high returns can only be achieved with high risk.

Online shopping fraud

If you have been conned by people misrepresenting goods or services online, either through auction or shopping sites you should:

- Keep all the correspondence and the goods involved.
- Use the online disputes section on the website concerned.
- Report it to Action Fraud.

Most online auction sites have substantial guidance and information for people buying and selling.

Make you sure you read and understand this guidance to avoid problems in the future.

Cheque overpayment fraud

Fraudsters overpay for goods or services with stolen cheques. Not only do the fraudsters get the goods without paying, they can also receive the excess money back from the seller.

To avoid this type of fraud never agree to accept overpayments for goods by cheque.

Types of fraud

Computer based fraud

There are a number of reasons criminals try to access your computer:

- To gain access to your personal details (name, address, phone number, date of birth, email addresses) to sell your personal details to other criminals.
- To use your computer or internet connection for illegal activity.
- To impersonate you to obtain goods or money.

Top tips:

- Don't be too trusting online – if you receive an email that looks unusual, delete it. Don't open hyperlinks in the email.
- Protect your computer, tablet or smartphone with anti-virus and anti-spyware (find out more from **www.getsafeonline.org**).
- Never reply to emails from people or organisations you don't know asking for your, or your company's, details. Never give someone passwords, no matter how genuine their request may seem.
- Use strong passwords for all your online accounts, for example, a minimum of eight characters with a combination of capital and lower case letters as well as numbers and symbols.
- Change passwords regularly.

Computer software service fraud

Fraudsters will call claiming to be from a well-known computer software company – like Microsoft or Apple – to encourage you to hand over credit card details for products or services you don't need. They might also try and access your computer to obtain personal information such as banking usernames and passwords, or to infect it with dangerous malware.

Some of the ways this fraud happens:

- Someone claiming to be from technical support calls to say they need remote access to your computer in order to fix it.
- You receive emails you didn't ask for with attached security updates to download.
- You are asked to supply credit card information to 'validate your copy of Windows'.
- You are told you have won the Microsoft Lottery.

Remember

Reliable computer firms do not:

- Call you to fix your computer if you have not asked them to. If you are suspicious, hang up and call your software provider using the contact number available on their official website.
- Send unwanted emails about security updates. Although they may send security software updates if you have subscribed to their security communications programme. If in doubt, don't open the email and call your provider to check.
- Ask for financial information over the phone to validate software such as Windows. **Never** give out personal or financial information over the phone or online.

There is no such thing as the Microsoft Lottery, so it is not possible you have won it.

Types of fraud

Mobile phone fraud

Some examples include:

- **Missed call/text fraud** – You get a missed call or receive a text from someone saying 'Hi, it's John. When do you want to catch up.' You text or call back only to find you are redirected to a premium rate service which can cost you up to £15.
- **Ringtone fraud** – You accept an offer for a 'free' or low cost ringtone. By accepting the offer you're actually subscribing to a service that keeps sending you ringtones and charging you a high rate for them.
- **Recorded message fraud** – You receive a message that you've won a prize. You call back on the number provided to find it is a premium rate number or your 'prize' will involve you spending more money.

Recovery fraud

If you have already been a victim of fraud you may be approached by someone pretending to be a lawyer, government official or enforcement officer. They will offer you an opportunity to recover your money. The fraudsters then try and get you to pay 'fees' to recover the money.

Top tips

- Be careful with companies contacting you about being a victim of fraud.
- If they sound genuine, ask them how they know you are a victim.
- Genuine agencies involved in fraud don't charge fees to return money to crime victims.
- Fraudsters sometimes use the names of genuine companies involved in fraud investigation to trick people. Check contact details you are given by unsolicited callers with the genuine company.
- Genuine companies do not normally use webmail addresses such as @yahoo or @hotmail.
- Overseas law enforcement agencies normally ask UK authorities to help return money, it is unusual for them to contact you directly.

Useful organisations

- Action fraud
  www.actionfraud.police.uk or 0300 123 2040.
  Report a crime or discuss a concern.
- Kent Crimestoppers
  www.crimestoppers-uk.org or 0800 555 111.
  Report crime anonymously.
- Cheatline
  www.insurancefraudbureau.org or 0800 422 0421. Confidential service to report insurance fraud.
- Citizens Advice Bureau
  www.citizensadvice.org.uk or 08444 111 444.
  Wide-ranging support on benefits, housing, employment, debt, consumer and legal issues.
- Which? Consumer Rights
  www.which.co.uk/consumer-rights guide to consumer rights.
- Kent County Council Trading Standards
  www.kent.gov.uk/tradingstandards
  Information on rogue traders and scams. Register for email alerts about scams, rogue traders and doorstep callers.
- Financial Conduct Authority
  www.fca.org.uk or 0800 111 6768. Financial regulator.
- BankSafeOnline (UK payments)
  www.banksafeonline.org.uk. Advice on payment fraud.
- The Money Advice Service
  www.moneyadviceservice.org.uk or 0300 500 5000. Information and advice on money matters.
- Cyber street wise
  www.cyberstreetwise.com a government campaign to support online safety.
- Get Safe Online
  www.getsafeonline.org
  Advice and information about online protection.
- Safer internet centre
  www.saferinternet.org.uk or 0844 381 4772.
  e-safety advice for children and young people.
- Financial Fraud Action UK,
  www.financialfraudaction.org.uk. Works with retailers, consumer and police to combat fraud.
- Think Jessica
  www.thinkjessica.com campaign to protect people from postal and telephone scams, particularly the elderly.
- Victim Support
  www.victimsupport.org.uk or 0845 389 9528.
  Free confidential support to anyone affected by crime.

FRAUD ISN'T JUST A SCAM
IT'S A CRIME

FRAUD ISN'T JUST A SCAM
IT'S A CRIME

Contact us:

Call **101** for non-urgent issues.
Call **999** in an emergency.

If deaf or speech impaired text '**Police**' and your message to **60066**

Facebook **'Kent Police'**
Twitter **@Kent_Police**

For more information and advice visit **www.kent.police.uk**

This leaflet is also available on request in large print and other formats. Please ring **01622 652158** for more information.