

# Fraud Prevention



## Key Points to Consider

- If it sounds too good to be true - it probably is
- Always be suspicious of cold calls
- Ask a friend or colleague for a second opinion
- Never agree anything in haste
- Don't do business on the doorstep

Fraud has become a common way for criminals to attempt to steal your money. This guidance note aims to make you aware of some types of fraud that are current, together with tips to help you stay safe.

## Payments, Loans, Lotteries and PPI Claims

The National Fraud Intelligence Bureau, is urging people to beware of fraudsters claiming to be from loan providers, lottery schemes, or from PPI claims companies.



Scammers will sometimes claim to have approved a loan and will ask for a fee to be paid in advance before it can be processed.



SUFFOLK  
CONSTABULARY

Alternatively, the scammers call to advise you that you are owed a PPI refund cheque for several thousand pounds, but again will for an administration fee in advance to receive this.

In some cases, residents have received letters through the post claiming that they have won a lottery, but fees or tax need to be paid before the winnings can be paid out.

The fraudsters then ask for the fee to be paid in advance with **UKash** vouchers.

Ukash codes can be purchased with cash from shops, petrol stations and kiosks, or are issued online from their website.

**Beware, you must not hand over Ukash codes to these scammers, as you will lose your money.**

No genuine loan company will ask for a fee to be paid in advance.



We have also received a number of other fraud reports from people who have used Ukash to pay for items purchased on auction sites which they have then not received.

Ukash should never be used for payments to unknown individuals. The simple message is to treat Ukash with the same security as you would physical cash.

Police often receive reports from people who have become victims of fraud in relation to PPI claims.

Citizens Advice is urging consumers to put the phone down on these cold callers and go straight to their bank to make a PPI claim. Claiming for mis-sold PPI is a free, simple process you can do yourself. For more information, contact your local Citizens Advice Bureau (CAB) or visit the Financial Conduct Authority's website.

[www.fca.org.uk](http://www.fca.org.uk)

### **Phoney Computer Maintenance Calls**

This is a common scam where the scammer rings the victim and states they are from a computer or technology company such as Microsoft or Virgin Media.

The caller explains that there is a problem with the victim's computer, for example that it has a virus. They then either go on to say they can fix the problem for a fee, or they persuade the victim to grant them



remote access to their computer.

This is where a person can control the computer from anywhere in the world, enabling them to copy personal files and data, including bank account details.

It also allows them to damage the machine, which they could then charge the victim to fix.

It isn't a particular group of people targeted by the offenders; people of all ages have been contacted and many people may not have reported being called. We are urging people to share the following advice:

- Computer firms, like Microsoft, do not make unsolicited phone calls and do not send unsolicited emails, requesting personal or financial

information or offering to fix people's computers.

- All unexpected calls and emails should be treated with suspicion and if you receive such contact you should hang up or delete the email.
- Never reveal your personal or financial details in these circumstances. Never allow anyone to remotely access your computer as they could access your personal data and files and cause damage to your machine.
- If you do need to contact the company for assistance or assurance, remember to contact them directly by using the details found on your contract or another trusted source.

Anyone who believes they may have been targeted by this scam or has information in relation to these incidents should contact the police via the non-emergency number 101.

### **Phoney Police Officer Telephone Fraud**

We continue to receive several reports each week from residents informing us that they have received phone calls from

fraudsters pretending to be bank or police staff investigating a fraud on their account and trying to convince them to provide their bank details and PIN or to move their money to a 'safe account' or to hand their cards or cash to couriers for safekeeping.



Although there have been a number of successful police operations where these fraudsters have been caught and convicted, others continue to operate.

Thankfully, most people are now aware of this type of fraud and have ended the call, however we still receive a small number of reports from residents who have provided their bank details or handed their money to the fraudsters.

Genuine police or bank staff would never ask you to withdraw or move cash from your account, nor would they ever ask you for your four digit bank card PIN number.

Beware that fraudsters sometimes ask their victim to type the PIN

into their phone so that it can be checked by an 'automated system'... but fraudsters have equipment which can identify which numbers the tones mean, so dialling it in is as good as saying it aloud.

If callers suggest that you call your local police or bank to check who they are, use another phone or ensure the line has been disconnected by phoning a friend or relative first or by waiting at least three minutes.

### **Donating To Charities**

Do not be put off giving to charities, they do really important



work, but be vigilant and take steps to make sure you are safely giving to legitimate charities. The Charity Commission provide advice, including:

- Fundraising materials should feature the charity's name, registered number and a landline contact number. Be wary of those that list only a mobile number. It is a legal requirement for UK charities with an income above £10,000 a year to provide their registration information on their documentation/website.

- You can search and check the charity's name, registration number and financial profile at the Charity Commission's website:

[www.charitycommission.gov.uk](http://www.charitycommission.gov.uk)



- Look for the FRSB tick logo indicating the charity is signed up to fundraising regulation, encouraging you to give with confidence. For details and advice about donating safely, visit [www.frsb.org.uk](http://www.frsb.org.uk)

### **Rogue Traders**

We often receive complaints about traders cold calling at the door and telling homeowners that their trees or roof or drains are unsafe and need work.

The work has then been badly done and often the price jumped dramatically because the trader 'helpfully' found other work that also had to be done!

We receive similar calls about driveway work, gardening and roof

cleaning. Although roof cleaning may make the tiles look cleaner, the force of the pressure washer can cause problems. The National Federation of Roofing Contractors advises that moss is not a problem on a roof and that this service is unnecessary.

Trading Standards advice is never to have work done by anyone who cold calls. No reputable trader ever approaches a customer in this way. If you think you need work, please use a recommended tradesman from friends/neighbours or contact the Citizen's Advice Consumer Service on 03454 04 05 06 to find a good trader on the Trading Standards Buy With Confidence list. Obtain three quotes to check if the price is competitive and if the work really needs doing - never rely on the word of a single trader.

Any contracts over £35 that are agreed in a consumer's home are subject to certain cooling off rights. The homeowner must be given written information about their right to cancel and about the identity of the trader who is doing the work. If that information is not given, the contract is unenforceable and the homeowner does not have to pay for any work done. Just having a

statement on a flyer or business card that there is a 7 day cooling off period is not enough.

If you need further help or advice please contact the Citizen's Advice Consumer Service on 03454 04 05 06.

### Find a Trusted Trader

The Suffolk Trader Scheme promotes the use of Checktrade's directory of local tradesmen who have been verified by Suffolk Trading Standards.



### Checktrade

<http://www.suffolk.gov.uk/community-and-safety/trading-standards-for-consumers/what-is-the-suffolk-trader-scheme/>

Checktrade is an online directory of local trades people who have been checked by Suffolk Trading Standards and are committed to treating their customers fairly.

### How it works

The Checktrade directory allows consumers to see what others have said about a trader, enabling

you to find the right tradesman for your needs.

In exchange for this free service, you will be asked to give feedback on traders for others to read.

The website has been running for over 15 years, and receives over 26,000 daily visits.

If you are unable to access the online directory please call 0845 408 4866.

You can also download the Checktrade app on your smartphone to find your nearest trader.

The best way to fight fraud and fraudsters is to get people talking about it and reporting it to **Action Fraud**.



If you have been a victim of fraud, there are two ways to report it to Action Fraud.

[www.actionfraud.police.uk](http://www.actionfraud.police.uk)

To report a fraud over the phone call: **0300 123 2040**

**Anyone witnessing a crime in action should call the police on 999.**



**If debit or credit cards, online banking or cheques are involved, your first step should be to contact your bank or credit card company.**

Reporting through Action Fraud ensures proper crime reporting procedures are followed, and in the case of fraud against you as a victim, you will be given a crime reference number.

Action Fraud are not able to recover money for victims; however trained agents can provide you with advice and guidance on getting support.

The information you provide will be referred to the National Fraud Intelligence Bureau, to be used in intelligence and investigation packages, and which may be forwarded to local police forces.

Although each individual report cannot be investigated, the information will help the police build up a picture of who is committing what fraud. This will help them stop the fraudsters and keep other potential victims safe.

Any information you have could help us prevent a crime. If in doubt, give us a call.

### **Call Blocking Services The Telephone Preference Service TPS**

The Telephone Preference Service is free of charge. You can opt out of many cold calls by registering with the Telephone Preference Service for free at [www.tpsonline.org.uk](http://www.tpsonline.org.uk) or by calling **0845 070 0707**.



Sir Robert Peel created the Metropolitan Police in 1829. He set out nine principles for policing. The First Principle was:

**“To prevent crime and disorder, as an alternative to their repression by military force and severity of legal punishment.”**

[Click here for further Crime Reduction Advice](#)



All your policing questions answered

<https://www.askthe.police.uk/content/>



**Secured by Design. (SBD)** The official UK Police flagship initiative combining the principles of 'Designing Out Crime' with physical security. We advise that you look on the SBD website for all of your Security products. <http://www.securedbydesign.com/>



More Security Products can also be found at:

<http://www.soldsecure.com/>

**CrimeStoppers.**  
Speak up. Stay safe.

Crime Stoppers is an Independent Charity that gives people the power to speak up to stop crime 100% anonymously <https://crimestoppers-uk.org/>

**0800 555 111**  
100% anonymous, Always



Help after crime—Contact Victim Support for free and confidential support

<https://www.victimsupport.org.uk/>

**Call us on 101. In an emergency always dial 999**

