



FRAUD PROTECT AND PREVENT

ADVICE FOR VICTIMS



NOTTINGHAMSHIRE
POLICE & CRIME
COMMISSIONER



NOTTINGHAMSHIRE
POLICE
PROUD TO SERVE

By reporting fraud, you will enable Nottinghamshire Police to build a picture of what type of fraud is being committed, this means that we can use our resources more effectively to prevent crime in the future.

In this booklet, please find advice and information which should give you more knowledge on how to protect yourself from scams, the current scam trends and to ensure you are not targeted in the future.

Please also share this information with family and friends to help protect them. Should you require any additional support from the Fraud Protect team, please contact us via nottsprotect@notts.police.uk.

Fraudsters will attempt to target you in a variety of ways, including via the telephone, online, on the doorstep and through the mail. There are steps you can take to protect yourselves and others from being targeted in these ways which have been included.

It's worth remembering that you'll never be contacted by a genuine organisation and asked to hand over money to a 'courier', asked for bank account or personal information or be requested to purchase vouchers / goods to assist with an investigation.

You should never feel ashamed or embarrassed about being targeted for any kind of scam. Our dedicated Nottinghamshire Victim Care support service 'Catch22' are here for you should you need further ongoing support due to this incident. Visit: www.nottsvictimcare.org.uk or Tel: [0800 304 7575](tel:08003047575).

Also please report any Fraud to [Reporting fraud and cyber crime | Action Fraud](#) or call them on [0300 123 2040](tel:03001232040).

Yours sincerely,
The Fraud Protect Team,
Nottinghamshire Police



Table of Contents

| | |
|------------------------------------|----|
| ● General Fraud Advice | 4 |
| ● Romance Fraud | 8 |
| ● Telephone Scams | 14 |
| ● Phishing Emails/Text | 18 |
| ● Messages Bogus Callers—Door Step | 21 |
| ● Mail Scams | 25 |
| ● Courier Fraud | 28 |
| ● Identity theft | 31 |
| ● Investment Fraud | 33 |
| ● Money Mule | 35 |
| ● Friend in Need | 38 |
| ● Safe Bank Accounts | 39 |
| ● Cyber Advice | 40 |
| ● Indemnity Claim | 44 |
| ● Reporting a Scam | 46 |
| ● Useful Organisations | 47 |

General Fraud Advice

Fraud is when trickery is used to gain a dishonest advantage, which is a financial gain for another person.

Fraud occurs by deception, someone will make contact claiming that they are from a genuine organisation, usually one that you use and will generally create a sense of urgency to therefore cloud your judgment.

There are many ways that a fraudster will contact you, this may be via the telephone, post, email or your social media accounts.

This information booklet ways to protect yourself and others from these types of frauds and scams.

Never:

Engage in conversations or respond directly to an email or text.

Contact the organisation using a number that you know to be genuine (don't press redial), use the telephone number on your bill of the back of your bank card and ensure that the line is completely disconnected for the fraudulent call, if possible, call from a different phone.

Replying to emails and confirm your details.

Genuine companies will never ask you to do this either via email or on the phone.

Provide bank account information, send or receive money.

NEVER give away your personal bank account information including sort code, account number or pin code no matter how convinced or scared you might feel.

Giving away any personal details online.

Revealing your full name, date of birth and home address may lead to your identity being stolen.

The below support will assist you in blocking unwanted calls:

Profile Location:

This could be a consideration depending on the provider.

Telephone Preference Service (TPS):

Free opt-out service for individuals who do not want to receive unsolicited calls. Tel: [0845 070 0707](tel:08450700707) or visit: www.tpsonline.org.uk

True Caller:

For smartphones you can download the True Caller app from any app store. Register your details & regularly update this to significantly reduce nuisance calls.

Call Blocker phones:

BT 4600 Cordless Nuisance Call Blocker phone is an example of what nuisance call blocking aids are available.

Make your phone number ex-directory:

To avoid having your phone number listed on websites, you need to contact your provider to have your number made ex-directory. This means your number won't appear in local telephone directories.

Network Provider:

These can provide services to reduce unwanted calls (this is separate to the TPS service) & you can also try requesting a limitation on international numbers if this facility isn't required.

Giff Voucher Scams:

NO legitimate debt can be paid in STEAM Cards / iTunes / Amazon vouchers – Hang-up on that call.

Neither the Police nor Banks will ever contact you to: Transfer money to a 'safe' account. Withdraw funds for safekeeping. Assist with an undercover investigation or collect cash, bank cards or PIN numbers.





FALL FOR THE PERSON, NOT THE PROFILE.

Stop. Taking a moment to stop and think before parting with your money or information could keep you safe.

Challenge. Is this person really who they say they are? Could their profile picture be fake? It's ok to refuse any requests for financial or personal details.

Protect. Contact your bank immediately if you think you've fallen for a scam and report it to Action Fraud on 0300 123 2040 or via actionfraud.police.uk. If you are in Scotland, please report to Police Scotland directly by calling 101.

ActionFraud
www.actionfraud.police.uk
TO STOP FRAUD

Romance fraud

Romance scams involve people being duped into sending money to criminals who will go to great lengths to gain trust and convince them that they are in a genuine relationship. They will use language to manipulate, exploit and persuade so that the requests for money do not raise alarm bells.

These requests will be highly emotive, such as the criminals claiming that they need money for things like emergency medical care, to pay for transport to visit the victim. Scammers will often build a relationship with their victims over a period of time.

Keep chatting on the dating site until you've met in person. Fraudsters want to quickly switch to social media / texting to avoid the site scam protection from detecting their grooming tactics & to hide their requests for money.

Be wary of excuses why the person can't video call or speak on the telephone. Fraudsters will often pose as someone working in either the military, or on an oil rig.

Beware of:

Anyone asking for personal details about you & your background but gives little information on themselves.

Vague communication around personal interests, they may repeat things or seem disconnected, dodge questions or make excuses for not meeting or speaking on the telephone.



The 'Sob Story':

Someone telling you how much they want to visit, but need a loan to pay for tickets / visas or for medical expenses for ill family members, discharge fees from their current job or for essential goods.

There's also the too good to be true business deal to be aware of, if only they had some extra up-front money to pay into this!

Beware of:

Repayment:

Any reference to gold / gems / diamonds as a repayment, allowing you to check a pretend bank online to show you a fake balance. Don't become a money mule.

Don't let time cloud your judgment:

Fraudsters use time to play their fake stories on you, make you believe the relationship is real, gain trust and all with one goal in mind, to financially exploit you, even if this is years down the line.

Declarations of love:

This can be within a matter of weeks, days or hours, so be cautious! You need to know someone to come to love them. Instant messages of love could be someone trying to get right into your life for all the wrong reasons.

Opening email attachments:

Don't - Especially from someone you have only just met.

Video Call:

Excuses to why the person can't video call. With internet cafés and technology around the world, there's never an excuse to prevent wvface-to-face communication where ever you are.

Profile names:

Different user name to that of the person you are speaking with. For example: User name - 'Davidin2u' and first message received states 'Hello how are you, my name is Kelvin.

Profile Location:

Discrepancies - location is in Malaysia but their profile states they're looking for a relationship in Germany.

Beware of:

Use only reputable dating sites and their own messaging service:

Ensure sites are part of the Online Dating Association (ODA).

Keep safe:

Do not share pictures or information about yourself or others that can give someone a hold over you. Your private life should stay private until you know that person, have met face to face and can start to trust them. Often victims can be socially engineered through social media accounts. To protect yourself, ensure you have all applicable security settings set to private preventing strangers from finding out everything about you.

Speak openly about your dating:

Use trusted friends or family (don't let embarrassment scare you). If you're involved emotionally it's hard staying objective. Alert them if a contact starts to feel strange, especially if the subject of money gets raised. If their advice is to back off, LISTEN! They have no emotional involvement and can provide the correct level of judgement with your best interests at heart.

Always

Account Security:

Be careful when accessing your account. Public or shared computers can be used to view or record your password or personal information. Keep your internet security software up to date.

Stop communicating if pressured over anything:

For personal or financial information or who seems to be trying to trick you into providing it or tell you to keep your relationship a secret. Never agree to this. This is a ploy to stop you telling your family and friends who have the opportunity to see this for what it really is.

User Names:

Choose a username that doesn't let everyone know who you are by not including your surname or anything that can identify you (place of work, family names or address).

Keep Contact Details Private:

Stay in control when it comes to how and when you share information. Don't include your contact information such as your email address, home address, or phone number in your profile or initial communications. Take things slowly and share more information when you feel comfortable doing so (especially after regular face to face contact). It is impossible to get back information once you have given it away and this can be used against you later on.

Never

Give away personal information

Revealing your full name, date of birth or home address. Giving this away may lead to your identity being stolen. If not advertised the fraudster will try using other conversational tactics to obtain this information from you (When is your birthday? How old are you?) This will give them your full date of birth.

Send or agree to receive money

The fraudster will try anything to get your bank details. Never do this no matter how much you trust them or believe their story, don't forget if they're genuine they wouldn't ask you for any money. If you do send money, they'll continue to come back for more until you have nothing left.

Assume fraudsters are illiterate

You are unlikely to see through the scam in an instant as you'd predict. Fraud / scamming is a pretty sick line of business but it is a business for them. They practice tugging at heartstrings, show tenderness and love, but can generally be needy and tell victims what they want to hear and can relate to.

Support available

Support Agencies to contact if you have been a victim of Romance Fraud: Age UK, Victim Care, Crime Stoppers, Action Fraud, Citizens Advice, Think Jessica and The Samaritans



Telephone scams

Phone scams are a common way for criminals to trick people into giving their personal details so that they can obtain money. Be aware of some of the most common phone scams and find out what you can do to stay safe.

Beware of calls where the caller says they are from your bank or the police about fraudulent use of your credit or debit card, or bank account. A scammer will ask you for all of your bank details including the number on the back of your card and your PIN, they may also tell you that you need to give your bank card to a courier. Neither your bank nor the police would ask you to do this.

You would also never be called by your bank or the police to move your money to a safe account due to your account being compromised. Pushy sales calls or investments that seem too good to be true.

Calls in relation to your computer. The person that is calling you may say that your computer has a virus, they will ask you to access your computer and download software to fix it, this is actually "Spyware" that will give the caller access to all of your online information and files that you have on your computer.

Be wary of any calls or text messages from stranger numbers offering products or services, such as pensions or debt management.

Callers stating that you are paying incorrect council tax banding or that you are entitled to a council tax rebate. Your council would never call you about a rebate, you can check your details online. Calls asking you to pay to renew a membership for Telephone Preference Services, this service is Free.

The Most Commonly used telephone scams:

HMRC

Victims are told they owe money to HMRC for outstanding tax. They may even be told there is a warrant out for their arrest. This scam creates a sense of urgency & panics victims into paying.

Courier Scams

Fraudsters will often pose as police officers. Victims are told there is a problem with their bank card & their assistance is needed in an undercover investigation & they need to withdraw money from the bank or hand over their card and PIN.

Tech support

Victims are told there is a problem with their computer. The fraudster then asks for remote access to the victim's computer to show them the 'errors'. Whilst they have remote access, they try to access the victim's online banking and transfer the victim's money to themselves.

Beware of

HMRC will contact you by letter, NEVER a call. NO legitimate debt can be paid in gift vouchers – HANG UP!

Don't trust your Caller ID. Fraudsters use a technique called 'spoofing', which allows them to 'hide' behind an authentic number, making a call appear genuine. They often use banks telephone numbers.

HANG UP & call the organisation on a genuine number, ensuring the line is fully disconnected. If possible, use a different phone. NEVER call back on the number given to you on the call.

The police & banks will NEVER call you & ask you for card or bank details, PINs, or to withdraw cash. You will never be asked to assist in an undercover investigation into the bank. They will never send someone to your home to collect cash or goods - HANG UP!

Microsoft / BT would NEVER call you in this way. NEVER allow remote access to your computer or other devices. HANG UP!

NEVER agree to download software called 'Team Viewer' off the back of a cold call.

Change Telephone Numbers: This could be a consideration depending on the provider

Telephone Preference Service (TPS):

Free opt-out service for individuals who do not want to receive unsolicited calls.

Tel: 0845 070 0707 or visit: www.tpsonline.org.uk

True Caller:

For smartphones you can download the True Caller app from any app store. Register your details & regularly update this to significantly reduce nuisance calls.

Beware of

Call Blocker phones:

BT 4600 Cordless Nuisance Call Blocker phone is an example of what nuisance call blocking aids are available.

Make your phone number ex-directory:

To avoid having your phone number listed on websites, you need to contact your provider to have your number made ex-directory. This means your number won't appear in local telephone directories.





Phishing emails/texts

Phishing is when fraudsters use scam emails, text messages or home calls to trick their victims, the aim is to make you visit a website, which may possibly download a virus onto your computer, or steal your bank details and other personal information.

Emails threatening a negative consequence, or a loss of opportunity unless urgent action is taken, are often phishing emails.

There are the things to look out for:

- Emails with bad grammar and spelling mistakes
- Emails with an unfamiliar greeting
- Inconsistencies in addresses and links
- Emails with suspicious attachments
- Emails requesting login details or payment information

Beware of

DPD / Other Couriers

Emails stating you have a missed delivery and there is a small charge for redelivery. Do not click the link! You do not have to pay to rearrange delivery.

TV Licensing

Emails stating your payment is due, or you're due a refund.

PayPal

Emails stating there is unusual activity on your account.

Amazon

Emails stating there is a problem processing an order & to click the link to confirm log in details.

Sextortion

Emails that claim to have accessed victim's devices following viewing pornographic websites.

HRMC

Emails stating you're due a tax rebate.

How to protect yourself

NEVER click on any links or attachments. Even 'unsubscribe' links can be malicious. Verify the email via a trusted source, such as logging into your Amazon / PayPal Apps directly to check any messages.

Use your spam filter. If you detect a phishing email, mark it as spam and DELETE.

The email address in the 'from' field is not guaranteed to actually be from that email address. Like telephone numbers, fraudsters can easily spoof email addresses to appear genuine.

Watch out for spelling or grammar errors like this in the subject field. This is an attempt to get around your spam filters.

Further information can be found at: <https://www.ncsc.gov.uk/collection/phishing-scams>

Report Phishing emails to report@phishing.gov.uk



Bogus Callers - Door Step Sales

Mail scams are sent by post and may be addressed to yourself with your name, they contain fake claims or offers that are designed to con you out of your money.

What to do

Traders

They might say that they have noticed something wrong with your property that they can fix.

Fake Police Officers

They could ask to see your bank card and ask you to tell them your PIN number.

Door to Door Sales

These people could be pushy offering large discounts and limited time offers.

Gas and Electric Personnel

People who claim to be from a gas or electricity company, but do not have any official ID.

Charity Collectors

Seem pushy or can not supply a registered charity number, asking you to sign up for a direct debit or make a standing order.

Joe Bloggs

A person/People who ask to come into your home saying that they need help, for example, they need to use your phone or they feel unwell or want to use the toilet.



What to do

You DO NOT have to open your door to anyone that you do not know, if you do, always think, Stop, Lock, Chain and Check.

STOP

Think, are you expecting anyone?

LOCK

If not, lock any other outer doors before answering the front door, as sometimes scammers work together.

CHAIN

Put the door chain on (but remember to take it off again or for people with access – a key – such as home help, children or your partner won't be able to get in), always look through the window or a spy-hole to see who is there.

CHECK

Ask for their identity, check the card for the business that they say they are from and check that the photo is of the person that is standing before you.

Get a telephone number off your bill or Google and use that number, not the number they give you.

Do not worry if you leave someone waiting, leave them outside of the property, not the inside and lock the door.

If you feel pressured or unsafe, contact friends, family or call the police on 101.

Mail Scams

Never buy from doorstep sellers.

Ask for a “no Cold Callers” sign from your local council or print one off from the internet and put it in the window.

Set up a password with your utility providers to be used by anyone they send around to your property so that you can be sure that they are genuine.

Do not be embarrassed to say “NO” or ask people to leave.

Never sign anything on the spot – take the time to think about any offer, do your research, even if it seems genuine at the time, where home improvements are concerned, it is always best to get several written quotes before deciding.

Don’t accept deliveries or anything you did not order that’s addressed to you. If you accept them without realising, contact the company they were sent from or your local police.

THINK: if it sounds too good to be true, it probably is.

Support can be obtained from Action Fraud and Citizens Advice who will contact Trading Standards, on your behalf.

Which.com has some good advice at: <https://www.which.co.uk/consumer-rights/advice/doorstep-scams-and-how-to-avoid-them-aWers5g-8JA3V>

To complain about a limited company visit: <https://www.gov.uk/complain-company>





Mail Scams

Mail scams are sent by post and may be addressed to yourself with your name, they contain fake claims or offers that are designed to con you out of your money.

Beware of

Lotteries, including foreign lotteries, or prize draws claiming you have won a fortune, these quite often look legitimate, with barcodes or ID numbers, the letter will then ask you to pay an administration fee, buy a product or call a premium rate phone number to claim your prize.

Psychics and clairvoyants who claim to have seen something in your future.

"Pyramid" investment schemes, these will ask you to pay a fee and recruit friends or family members to get a return on your investment.

Begging letters, people asking for money because of unfortunate circumstances, like an illness or poverty.

Letters addressed from a "solicitor" about unclaimed inheritance, often from a "relative" that you have never even heard of.



What to do

Reject and Ignore

If you receive a letter that you think is a scam, ignore it, do not call any telephone number, numbers that start with an 09 cost you up to £4 per minute.

Report

Join a mail marshal scheme, you send them your Scam mail so that they can catch the scammers.

Verify

If you are unsure check the details of the organisation or solicitor online (ask a family or friend if you do not have the internet).

Opt Out

Try to avoid being added to mailing lists, for example when you register to vote, tick the Opt Out of the edited register (this is also known as the open register) as this can be used to sell on your details thus the increase in unsolicited "Junk Mail".

Reduce your Junk Mail

Register with a mailing preference service, this will put an end to mail from the direct mailing companies contacting you, this will reduce, not stop all of them. Unfortunately, it is not easy to control what people send you, but you can control your answer.

Who to contact:

- Tell Royal Mail if you think you have received scam mail and send it directly to them with a covering letter.
- Report details of overseas scams to Citizens Advise.

Courier Fraud

Courier fraud is when a fraudster contacts the victim by telephone pretending to be a police officer or bank official. The caller might be able to confirm some basic details about the victim such as their full name and address.

The caller may also offer a telephone number for the victim to call back on. In these circumstances, either the number offered will not be genuine or, where a genuine number is suggested, the fraudster will stay on the line and pass the victim to a different individual.

Beware

After some trust has been established, the fraudster may suggest; Some money has been removed from a bank account and staff at their local bank branch are responsible.

"Pyramid" investment schemes, these will ask you to pay a fee and recruit friends or family members to get a return on your investment.

Suspects have already been arrested but the "police" need money for evidence.

A business such as a jewellers or currency exchange is operating fraudulently and they require assistance to help secure evidence.



How to protect yourself

The Police or the Bank will NEVER contact you out of the blue.

The police nor the bank will NEVER send anyone to collect your Bank Card from you.

They will also NEVER do the following: -

- Inform you that you are needed as part of an undercover investigation.
- Ask you to attend your Bank and withdraw large sums of money or buy expensive items like Rolex Watches or purchase gift cards.
- No bank will have counterfeit money in their branch.
- Neither the Police nor the Bank will ever send a "Courier" to collect money, goods, gift cards or your bank card.

Should you receive any call like this, immediately hang up the phone, use a different phone if possible, or wait 10 minutes, then call your bank with the number that is on the back of your bank card, or the Police on 101.

Never press redial.

Alternatively call a trusted person, like a family member or neighbour. This advice is recommended for any call that is not Family or Friends unless you are expecting a call back in relation to a previous conversation.

Advice is available from Crimestoppers, Action Fraud, Citizens advise, Age UK, your local bank.

How it happens

You may get called on your mobile or landline by someone who claims to be from your bank or the police. They say their systems have spotted a fraudulent payment on your card or it is due to expire and needs to be replaced.

They might suggest that you hang up and redial the number of their bank or police force to reassure you that they're genuine. However, they don't disconnect the call from the landline so that when you dial the real phone number, you're still speaking to the same fraudster.

They'll then ask you to read out your credit or debit card PIN or type it on your phone keypad. They may ask for details of other accounts you hold with the bank or elsewhere to grab more information.

Then they promise to send a courier to you to collect your bank card. The fraudster will have your name, address, full bank details, card and its PIN, and withdraw cash using the card and may even use the information to commit **identity fraud** in your name.





Identity Theft

Identity Theft

Your name, address and date of birth is enough information for create another "you". An ID thief can use several methods to find out your personal details and use this information to open bank account, apply for loans, take out credit cards and apply for Benefits in your name. Below are a few signs to look out for that might mean you have been or may become a victim.

Important Documents lost, like your driving licence or passport, you must contact the passport office or the DVLA as soon as you realise that these documents are missing. Mail from our Bank or Utility company, external post boxes offer the opportunity for mail to be stolen and then for other mail relating to say bank accounts that have been set up to be taken also. Transactions appear on your bank statement that you do not recognise, contact your bank, and have the card frozen, explain to them that you are not aware of these transactions.

You are refused Loans or Credit cards despite having a good credit history. Check your credit account via Experian, Clear Score etc. You receive letters in your name from Debt Collectors or solicitors for debts that are not yours, contact these companies as soon as possible, and also check your credit score.

Use credit reference agencies to check your details, also register with CIFAS at: <https://www.cifas.org.uk/services/identity-protection/protective-registration/application-form>

How to protect yourself

- Don't throw out anything with your name, address or financial details without shredding it first.
- If you receive an unsolicited email or phone call from what appears to be your bank or building society asking for your security details, never reveal your full password, login details or account numbers. Be aware that a bank will never ask for your PIN or for a whole security number or password.
- If you are concerned about the source of a call, wait five minutes and call your bank from a different telephone making sure there is a dialing tone.
- Check your statements carefully and report anything suspicious to the bank or financial service provider concerned.
- Don't leave things like bills lying around for others to look at.
- If you're expecting a bank or credit card statement and it doesn't arrive, tell your bank or credit card company.
- If you move house, ask Royal Mail to redirect your post for at least a year.

These credit reference agencies offer a credit report checking service to alert you to any key changes on your credit file that could indicate potential fraudulent activity:

- TransUnion
- Equifax
- Experian
- ClearScore
- Noddle

It is particularly helpful to check your personal credit file 2-3 months after you have moved house.



Investment Fraud

Investment Fraud usually involves criminals contacting people out of the blue and convincing them to invest in schemes that are actually worthless or do not exist. Once the criminals have received a payment they will cease contact with the victim.

If you're contacted out of the blue about an investment opportunity, chances are it's a high-risk investment or a scam. Scammers usually cold-call but contact can also come by email, post, social media, word of mouth or at a seminar or exhibition. Scams are often advertised online too.

If you get cold-called, the safest thing to do is hang up. If you get unexpected offers by email or text, it's best to simply ignore them. Follow our telephone guidance for information on how to reduce unwanted telephone calls.

Callers may pretend they aren't cold - calling you by referring to a brochure or an email they sent you - that's why it's important you know how to spot the other warning signs.

Spot the warning signs:

Unexpected contact

Traditionally scammers cold-call but contact can also come from online sources e.g. email or social media, post, word of mouth or even in person at a seminar or exhibition.

Time pressure

They might offer you a bonus or discount if you invest before a set date or say the opportunity is only available for a short period.

Social proof

They may share fake reviews and claim other clients have invested or want in on the deal.

Unrealistic returns

Fraudsters often promise tempting returns that sound too good to be true, such as much better interest rates than elsewhere. However, scammers may also offer realistic returns in order to seem more legitimate.

False authority

Using convincing literature and websites, claiming to be regulated, speaking with authority on investment products.

Flattery

Building a friendship with you to lull you into a false sense of security.

Remote access

Scammers may pretend to help you and ask you to download software or an app so they can access to your device. This could enable them to access your bank account or make payments using your card.

Do your research into the company that you are about to invest in, you can check these out on the FCA website. Double check details such as email addresses, that can look very similar, and check for punctuation.

Easy Money with no strings attached?

Money Mule

Criminals may ask you to receive money into your bank account and transfer it into another account, keeping some of the cash for yourself. If you let this happen, you're a money mule. You're involved in money laundering, which is a crime.

You might be approached by criminals online or in person. They might post what looks like a genuine job ad, then ask for your bank details.

Once you become a money mule, it can be hard to stop. You could be attacked or threatened with violence if you don't continue to let your account be used.

Don't Be Fooled by offers of quick cash.

Criminals need money mules to launder the profits of their crimes. Mules will usually be unaware of where the money comes from – fraud, scams and other serious crime – or where it goes.



Your bank account will be closed.



You will find it hard to access further student loans.



It will be difficult to get a phone contract.



You will have problems applying for credit.



You could go to prison for up to 14 years.

What is a money Mule?

Money Muling is a type of Money Laundering, Money Laundering is to disguise where money of crime has really come from, i.e. by moving money through multiple bank accounts. Criminals will recruit people – known as money mules to do this.

Some victims do not know that they are being used as money mule, maybe a friend or online partner has asked you if they could have some money transferred into your bank account as theirs “is locked” and for you to then forward this on to another “mate” that they owe money to.

It could be possible that you have been sent cash in the post and that you need to send this on to another person, you could have been asked to do this after receiving a phone call, out of the blue, claiming that you have PPI due to you and you have to pay a fee, or that you are owed money back from an overpayment of a loan or mortgage and again you have to pay a fee.

Money Laundering is a criminal offence, your bank accounts could be closed etc.

Always say no if someone asks you to use your bank account, should you receive funds, do not send them on, inform your bank.

Parcel Mules to run with money Mules

Sometimes a fraudster may send you a parcel, with instructions to forward it on without opening it. It is likely that the contents are a result of criminal activity and therefore you may be facilitating crime by sending this on to another person.

Should you be asked by someone if they can send a parcel to your address and for you to send this on, refuse. Should you receive an item, call the police on 101.

Friend in Need Scam



This all starts with a WhatsApp or a text message from an unknown number, the message starts "Hi Mum" or "Hi Dad", with a message that usually states "I am texting you off a friend's phone as I have smashed mine/dropped it down the toilet, please can you text me on my new number as this phone is about to die."

A conversation starts, you believe that this is your child. After a couple of messages, they then tell you that they have a bill that they need to pay and can not access their banking app on their new phone, they ask if you would pay this for them and state that they will send you the money back as soon as they can.

You may only realise that it's a scam when they don't answer the phone or say something in a message that seems out of character.

These messages are from Fraudsters, if you receive a message like this, do not reply or engage in any conversation. Call the person you believe it to be on the number that you have for them.

Safe Bank Accounts

You receive a call from someone saying that they are from your bank and that your bank account has been compromised. They could say that there has been some fraudulent activity on your bank account and that to safeguard your money, you need to move this to a "Safe Account" which the caller says they have set up for you.

You transfer all your funds, into the Safe Account, to later find out that you have no access. The bank will never call you to say that your bank account has been compromised.

If you do receive such a call, hang up the phone and use a different line to call your bank, if you do not have a different line, wait 10 minutes and call the bank using the telephone number on the back of your card or a letter, do not use redial as the fraudsters will have spoofed the telephone number and you will be calling them back.

Cyber Advice

If you think you have downloaded a virus

Consider having your computer looked at by a trusted technician in order to determine if malicious software was installed on your machine during the call. For advice on how to recover an infected device please visit: www.ncsc.gov.uk/guidance/hacked-device-action-to-take

Always question unsolicited calls, texts or emails requesting your personal or financial information (Name, address, bank details, email or phone number).

If you are concerned about any unauthorised or unusual transactions requested via your bank, please hang up and contact your bank directly using a known email or phone number identified through official paperwork you have received in the past. If you're unsure of a caller's identity, hang up. Even if the caller can provide you with details such as your full name, don't give out any personal or financial information during a cold call.

Report any identification that may have been accessed from your device as stolen.

You can also check with HMRC and the electoral register to ensure your details haven't been changed. For example, address details.

- Passport: Passport photo or copy of passport sent – Tel: 0300 222 0000
- Driving licence: If this is compromised, contact your insurance company and the DVLA.
- National Insurance number: Contact the Inland Revenue/HMRC to confirm the compromise. Tel: 0300 200 3500 (Mon - Fri: 8am to 8pm & Sat: 8am to 4pm)

Two-Factor Authentication (2FA) - This can also be referred to as 'two step verification or multifactor verification (2SV)'.

- Two factor authentication (2FA) greatly increases the security of your account, even if they have your password.
- For more information visit: www.ncsc.gov.uk/cyberaware/hom

Enable strong privacy settings:

Social Media:

- Approve who follows you and what you get tagged in.
- Disable/hide your email address and mobile number from linking to your social media accounts within a search engine.
- Change your settings to 'hide' your friends/followers to protect yourself from falling victim to account impersonation, these are set up to bypass privacy settings and target friends/followers with targeted scams. Remove unused connected devices that are no longer required.
- Think about what personal information is stored. For example. Your full date of birth.
- Don't let the world know your location, do this by disabling your location'. Use a different password for each social media account.
- Ensure your linked email is up to date, having an old email leaves your account at risk and will make it difficult if you ever need to recover the account.

For further information on these settings:
www.eastmidlandscybersecure.co.uk/general-5

Computer Service Software Fraud

- This occurs when fraudsters posing as legitimate companies, such as your internet service provider (ISP) or Microsoft, call to tell you that there's a problem with your computer.
- They'll say something like: There's a virus on your computer, There is something wrong with your computer or Your router or internet connection are not performing properly.
- They might say that they can fix the problem for a fee, or alternatively they can compensate you for the problem you are experiencing. What these fraudsters really want is for you to unwittingly grant them remote access to your computer by installing software or visiting a particular website, and for you to give them your payment details.

What can be done about it

- The majority of these frauds are carried out overseas through international call centres, but by reporting such calls to Action Fraud, important intelligence can be gathered, and preventative action can be taken by the police. For example, suspending telephone numbers and websites used to commit this type of fraud.
- Legitimate companies like Microsoft, Amazon, Virgin, Sky, BT and Google will never cold call you are asking for remote access to your computer or for your financial details.
- Take the time to think about the documents, data, and identification on the device, did you have a copy of your passport, drivers' licence or other personal details on your computer and ensure you follow the identity advice below.
- Notify your bank if financial payment has been taken or made and you believe it to be a scam

How to protect yourself

Removing software

Remote access can be gained using genuine remote access software tools, but these can be used with malicious intent in the event of a scam. Examples of remote access tools are AnyDesk, TeamViewer, Quick Support, Zoho Assist and more. These are genuine software companies.

It is important to uninstall anything that you recall downloading or has appeared. If you feel confident and able to do so you can attempt to uninstall any remote software applications yourself, alternatively please speak to friends, family, or a local computer expert (please do your research first), to help you with this. Below is an example of how to uninstall software using the Control Panel (for programs) on a windows computer or laptop:

In the search box on the taskbar, type Control Panel and select it from the results.

- Select Programs > Programs and Features.
- On the 'Installed on' click this to organise installed applications in date order
- Go to the software dated the same date as the incident occurred (the date the access was first granted to your computer).
- Press and hold (or right-click) on the program you want to remove and select Uninstall or Uninstall/Change. Then follow the directions on the screen.
- For further advice and support visit: <https://support.microsoft.com/>

If you think you might have been a victim of Cyber-Crime

Please visit: www.actionfraud.police.uk or call: 0300 123 2040, to report the incident. Alternatively, if you are currently being subjected to a live and ongoing cyber-attack then please contact us on 101.

To report a fraudulent email

These can be forwarded to the National Cyber Security Centre inbox: report@phishing.gov.uk or for text scams forward the original message to 7726 (spells SPAM on the keypad).

Report a scam website: www.ncsc.gov.uk/section/about-this-website/report-scam-website



Indemnity Claim

If you have been a victim of Fraud, there may be a possibility that you could receive funds back, this is only with the bank that you have transferred the funds from.

In the first instance, call your bank and ask to speak to the Fraud Department, ensure that you have all your account details to hand of the account that you transferred the monies from.

Once you are through confirm to the operator that you are calling as you have been a victim of Fraud, confirm the details to the operator, i.e, if it was a Romance Scam, confirm the amount of time that you have been in a relationship, where they live, why they have asked for money, the account details of the person including the Sort Code, Account Number and Name of the Person.

Advise of any threatening behaviour, for example, if you did not do as they said then they know where you live, if you do not pay as and when stated they are a Police Officer from a Force outside of the local area and if payment is not going to be made then you will be arrested.

Your bank will advise you that they will need to investigate your case and will advise you once they have investigated.

Once you have received your banks decision and if they state that they will not be refunding any monies to you, then you should call your bank account, speak to the Fraud Department, and confirm that you wish to raise a Formal Complaint, again you will have to explain the details as pervious.

Again, the bank will review this and then get back to you with their decision.

If the bank again refuses the refund your funds, then you can take your case to the Financial Ombudsman, you can complete a form online which is very self-explanatory.

Reporting a Scam

Reporting a scam If you've been the victim of scam, here are some tips on what you should do next:

It's nothing to be embarrassed about. Scams can, and do, happen to anyone. Don't be ashamed

First call your bank, then Action Fraud If you've lost any money in a banking fraud, the first thing you should do is get in touch with your bank so they can cancel any cards or freeze your account.

Then, contact Action Fraud. Your experience could help others. The information you provide could help authorities track down the scammer, making them pay for their crime and protecting others.

You might even get some money back. This can't be guaranteed unfortunately, but it may be possible in certain circumstances:

- If you paid for something by credit card in a transaction that turns out to be fraudulent, your card provider may offer protection.
- If you have household insurance, your policy may also provide cover in some circumstances.
- If the scammer is traced, it may be possible to prosecute them and recover your money. Get advice whenever you're unsure.

Be cautious if you're approached by someone claiming to help scam victims recover their money – this could also be a scam. Contact the Citizens Advice consumer service.

Top tips to remember


No one expects you to memorise all the advice in this guide. So here's a handy summary of top tips to help you stay safe.

Who to contact for further help:

- Action Fraud – to report a scam – 0300 123 2040
- Citizens Advice consumer service – 03454 04 05 06

Useful Organisations




-  Action Fraud is the national reporting service for fraud and cybercrime in England, Wales and Northern Ireland. Fraud can be reported online or by phone. The website also provides information, guidance and advice on different types of fraud.

 www.actionfraud.police.uk

 0300 123 2040

 0300 123 2050



-  UK Nottingham & Nottinghamshire is the largest local independent charity providing a wide range of services for older people and for over 80 years it's been our mission to improve their lives.


Age UK Notts can offer telephone-based support from 9am – 5pm Monday to Thursday and 9am – 4.30pm on Fridays.

 <http://www.ageuk.org.uk>

 0115 844 0011




**citizens
advice**

 Free, independent, confidential and impartial advice online, over the phone or in person.

 www.citizensadvice.org.uk

 0800 144 8848



 The Met Police produce advice covering many aspects of fraud and cyber crime. Find our guides and videos here:

<https://www.met.police.uk/littlemedia>


 www.met.police.uk



 Helping organisations and the general public in the UK with cyber safety.

 www.ncsc.gov.uk



 Made up of three leading charities, the UK Safer Internet Centre provides online safety support, resources and services to children and young people, adults facing online harms, professionals working with children, and parents and carers.

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



Solicitors
Regulation
Authority

- ① The Solicitors Regulation Authority is the regulator of solicitors and law firms in England and Wales. On their website, you can find details of how to check if a solicitor or law firm is regulated, and how to make a report. There is also a section on their website which has scam alerts.

🌐 www.sra.org.uk

☎️ 0370 606 2555



TO STOP FRAUD™

- ① Take Five is a national campaign that offers straightforward and impartial advice to help everyone protect themselves from financial fraud.

Led by UK Finance, the campaign is delivered with and through a range of partners in the UK payments industry, financial services firms, law enforcement agencies, telecommunication providers, commercial, public and third sector organisations.

🌐 <https://takefive-stopfraud.org.uk>



- ① StepChange is the UK's leading debt charity to get expert advice and fee-free debt management.

Open to calls from 8am to 8pm.

🌐 <http://stepchange.org>

☎️ 0800 138111



- i** You can escalate complaints using this service if you're unsatisfied with how your bank or building society has treated you after you've reported a scam.

 www.financial-ombudsman.org.uk

 0800 023 4567



- i** MoneyHelper is here to make your money and pension choices clearer. Here to cut through the complexity, explain what you need to do and how you can do it. Here to put you in control with impartial guidance that's backed by government and to recommend further, trusted support if you need it.

 www.moneyhelper.org.uk

 Pensions Helpline: 0800 011 3797
Money Adviceline: 0800 138 7777



- i** Friends Against Scams is a National Trading Standards Scams Team initiative, which aims to protect and prevent people from becoming victims of scams by empowering people to take a stand against scams.

Learn how to protect yourself and your loved ones from scams by completing the Friends Against Scams awareness session and help to raise awareness throughout your community.

Anybody can join Friends Against Scams and make a difference in their own way. The organisation offers information and schemes such as the Scam Marshal' scheme.

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

 01323 463600

 friendsagainstscams@surreycc.gov.uk



i Like telephone, email and online scams, there are a few different types of scams that can be sent in the post. Sometimes they are tricky to spot. We want to help you look out for scam mail and explain how you can avoid falling victim to it.

What is scam mail?

Scam mail can take the form of fake lotteries and prize draws, get-rich-quick schemes, bogus health cures, investment scams and pyramid schemes. Sometimes these can be sent to you if a scammer has got hold of your contact details fraudulently.

What to do if you think you've received scam mail

If you think you or a family member is receiving scam mail, please complete our dedicated form at <https://www.royalmail.com/reportingscammal>

In addition you can post your letter directly to FREEPOST SCAM MAIL.

 www.royalmail.com

 [0800 0113466](tel:08000113466) (Message service only)

 scam.mail@royalmail.com

For more fraud tips & scam alerts:

Follow us on:



@NottsFraudCops



@NottsPolice



Nottinghamshire Police



NOTTINGHAMSHIRE
POLICE
PROUD TO SERVE



