

Fraud

Protect and prevent advice

NOTTINGHAMSHIRE
POLICE
PROUD TO SERVE

THINK FRAUD

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

In this booklet you will find advice and information on how to protect yourself from scams. There is a useful list of support organisations at the end of this booklet.

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 in this booklet.

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** is here for you should you need further ongoing support due to this incident.

Visit: www.nottsvictimcare.org.uk or Tel: 0800 304 7575.

Report any fraud to Action Fraud via: https://www.actionfraud.police.uk/reporting-fraud-and-cyber-crime or call them on 0300 123 2040.

Yours sincerely,
The Fraud Protect Team,
Nottinghamshire Police

Contents

Romance fraud 4

Telephone scams 6

Phishing emails/texts 10

Bogus callers - doorstep sales 13

Mail scams 17

Courier fraud 19

Identity theft 21

Investment fraud 23

Money mule 25

Friends in need 26

Indemnity claim 27

Cyber advice 28

Other frauds 32

Useful organisations 35

Checklist 40

Romance fraud

Romance scams involve people being manipulated into thinking they are in a romantic relationship and sending money to fraudsters who will go to great lengths to gain trust. They will use language to persuade and convince so that their requests for money do not raise alarm bells.

These requests will be highly emotive. Fraudsters claim they need money for things like emergency medical care or to pay for transport to visit the victim. Fraudsters will often build a relationship with their victims over time.

Fraudsters will want to quickly switch to social media / texting to avoid the dating site scam protection from detecting their grooming tactics and to hide their requests for money.

Be wary of excuses when the person can't video call or speak on the telephone. Fraudsters will often pose as someone working in remote locations where contact can be problematic such as the military or on an oil rig.

Beware of:

- Anyone asking for personal details about you and your background but gives little information about themselves.
- Vague communication around personal interests, excuses for not meeting or speaking on the telephone.
- Someone telling you how much they want to visit, but need a loan to pay tickets, visas, medical expenses for ill family members, discharge fees from their current job or for essential goods.
- Fake celebrity profiles. Actual celebrities will not contact you via Social Media
- Profile names being different to the name of the person you are speaking to online. For example user name 'Davidin2u' and first message received states "Hello how are you, my name is Kelvin".

Use only reputable dating sites and their own messaging service.
Ensure sites are part of the Online Dating Association (ODA).

Keep safe

Your private life should stay private until you know that person, have met face to face and can start to trust them. 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 put you off). If you're involved emotionally, it's hard to stay objective. Alert them if a contact starts to feel strange, especially if the subject of money is raised. If their advice is to back off, LISTEN! They have no emotional involvement and can provide a level of judgement with your best interests at heart.

Support available

Here are some support agencies to contact if you have been a victim of romance fraud:

Age UK Nottingham and Nottinghamshire

Nottinghamshire Victim Care

Lovesaid

Action Fraud

Citizens Advice

Think Jessica

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. Beware of some of the most common phone scams and find out what you can 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 your bank details including the number on the back of your card (the CVV) 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 will never be called by your bank or the police to move your money to a safe account due to your account being compromised.

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

Be wary of callers stating that you are paying incorrect council tax 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. Be wary of 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 is designed to create a sense of urgency and panic.

Courier scams

Fraudsters will sometimes pose as police officers or bank officials. Victims are often told there is a problem with their bank account, or their assistance is needed in an undercover investigation. Victims may be asked to withdraw money from the bank or hand over their card and PIN to a courier.

Technical support

The person may call you to say that your computer has a virus, they will ask to access your computer and download software to fix it, this may be “Spyware”. This will give the fraudster access to everything in your computer including your apps, emails and contacts and your online banking.




DON'T ASSUME
A PHONE CALL IS
AUTHENTIC
JUST BECAUSE
SOMEONE KNOWS YOUR
NAME AND ADDRESS
ActionFraud
POLICE

Beware of:

- Calls proporting to be from HMRC, they 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 authenthic number, making a call appear genuine. They often use banks' telephone numbers.
- HANG UP and 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 and banks will NEVER call you and ask you for card or bank details, PINs, or to withdraw cash. You will never be asked to assit in an undercover investigation into the bank. They will never send someone to your home to collect cash or goods - HANG UP!
- NEVER agree to download any software onto your device off the back of a cold call.



Telephone preference service

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 app

For smartphones you can download the True Caller app from any app store. Register your details and 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.

Changing your telephone number may also be a consideration.



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.

These 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
- Emails with unusual characters in the domain e.g. info@companyname-mai-department.com



Beware of:

Couriers/delivery companies

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

TV Licensing

Your payment is due, or you're due a refund.

PayPal

There is unusual activity on your account.

Amazon

There is a problem processing an order and to click the link to confirm log in details.

Sextortion

Claim to have accessed a victim's devices following viewing pornographic websites.

HMRC

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 spe11ing oR grAmMar ErR0Rs L1Ke 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 - doorstep sales



Beware of:

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 cannot 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 have 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 for people who have access with a key - such as home help, children or your partner as they 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 an official telephone number off your bill or the internet 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.

What to do

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 to 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.

Citizens Advice:
https://www.citizensadvice.org.uk/consumer/scams/reporting-a-scam/

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 you with your name. They contain fake claims or offers that are designed to con you out of your money.

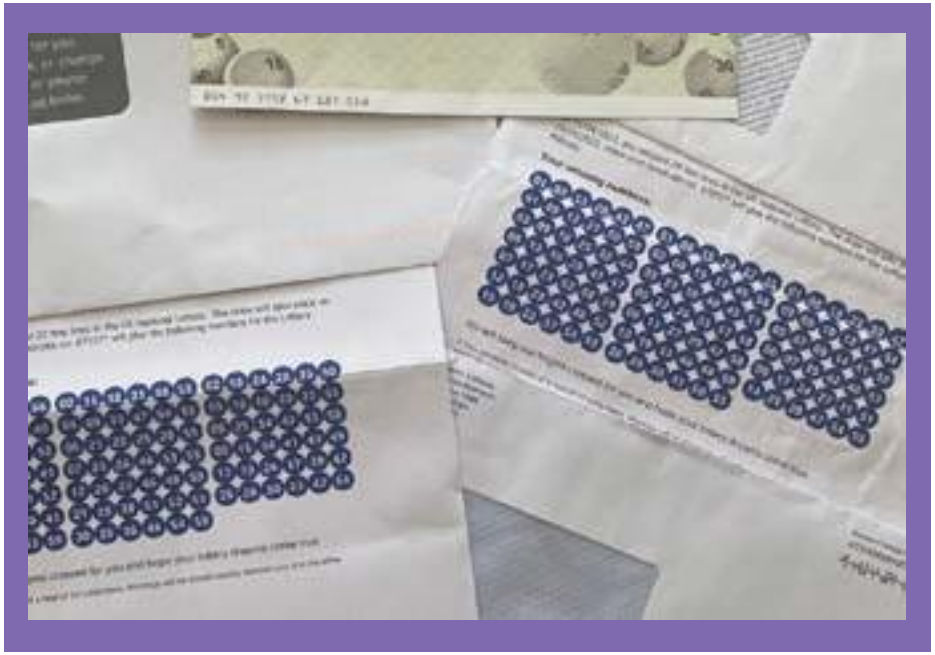
Beware of:

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 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.

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 recieve 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, where you send them your scam mail so that they can catch the scammers.

Verify

If you are unsure, check the details of the organisation online (ask a family member 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 but 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 recieved scam mail and send it directly to them with a covering letter.

- Report details of overseas scams to Citizens Advice.

Impersonation fraud

You may get called on your mobile or landline by someone who claims to be from your bank or the police. They may say their systems have spotted a fraudulent payment on your account, card or perhaps your card is due to expire and needs to be replaced. They may say that they need your help to investigate a crime and ask you to withdraw cash from your bank.

They might suggest that you hang up and re-dial 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 or cash. The fraudster will have your name, address, full bank details, card and its PIN, and withdraw cash, use your card to make purchases or may even use the information to commit identity fraud in your name.

Beware of:

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

Fraudsters may say that a suspect has already been arrested but the "police" need money from the bank for evidence.

Fraudsters may even ask you to go to a business such as a jeweller or currency exchange as they believe it 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 an expensive item or purchase gift cards
- No bank will issue counterfeit money
- Neither the police nor the bank will ever send a “courier” to collect money, goods, gift cards or your bank card, and PIN.

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 re-dial.

Alternatively call a trusted person, like a family member or neighbour for advice.

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

Identity theft

Your name, address and date of birth is enough information for fraudsters to create another “you”. An ID thief can use several methods to find out your personal details and use this information to open bank accounts, 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.

If you lose important documents like your driving licence or passport, you must contact the passport office or the DVLA as soon as you realise they are missing.

If transactions appear on your bank statement that you do not recognise, contact your bank and have the card frozen.

If you are refused loans or credit cards despite having a good credit history, then check your full credit account via an approved credit referencing company. If you receive letters in your name from debt collectors or solicitors relating to debts that are not yours, contact these companies as soon as possible.

You can also 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, who will put a fraud marker on your accounts.



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 mintues and call your bank using a trusted phone number, from a different telephone, if possible
- 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 or a new card 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

The below 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

Noodle

It is particulary 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 encourage further payments or request a fee to release your funds.

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, **hang up**. If you get unexpected offers by email or text, simply ignore them.

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

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, add fake celebrity endorsements and claim other clients have invested or want in on the deal to encourage people to invest.

Unrealistic returns

Fraudsters often promise tempting returns that sound too good to be true. **IT IS**.

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 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 (Financial Conduct Authority) website https://www.fca.org.uk/

Money Mule

Money muling is a type of money laundering. Money laundering is a method of disguising where money from crime has come from by moving money through multiple bank accounts. Criminals will recruit people – known as money mules to do this.

Some people do not know that they are being used as a 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 person.

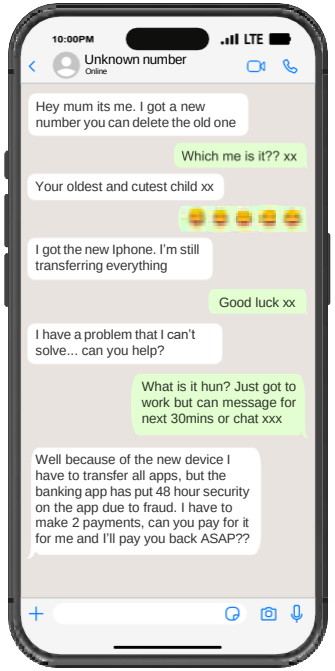
It could be possible that you have been sent cash in the post and that you need to send this on.

Money laundering is a criminal offence, your bank accounts could be closed if you are suspected of laundering funds. You could have problems getting credit in the future and this could also affect your credit rating.

Always say no if someone asks you to use your bank account. If you are sent funds do not send them on. Instead inform your bank.



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.”

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 cannot 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 the fraudster is purporting to be on the number that you have for them to check the veracity of the message.

Indemnity claim

If you have been a victim of fraud, there may be a possibility that you could receive funds back. This is only available 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.

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

If your bank decides they will not be refunding any monies to you, then you should call your bank, speak to the fraud department, and confirm that you wish to raise a formal complaint.

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

If the bank refuses to refund you, then you may able to take your case to the Financial Ombudsman by visiting https://www.financial-ombudsman.org.uk/make-complaint.



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).

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.

- Stolen or Missing Passport: Passport photo or copy of passport sent Tel: 0300 222 0000 or visit: https://www.gov.uk/report-a-lost-or-stolen-passport
- Driving licence: If this is compromised, contact your insurance company and the DVLA or visit: https://www.gov.uk/replace-a-driving-licence
- National Insurance number: Contact the Inland Revenue/HMRC to confirm the compromise. Tel: 0300 200 3500 (Mon - Fri: 8am to 8pm and 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/home

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 becoming a 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 clicking 'disable 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:
https://www.eastmidlandscybersecure.co.uk/resources

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, laptop, tablet or mobile.

They'll say something like: "There's a virus on your computer", or "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.

Companies may call you for a legitimate reason so take care when you are contacted out of the blue. It is best to disengage when contacted and call the company back on a number you know is genuine to speak to a member of staff.

Treat these as you would a cold caller turning up at your door. 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?

Notify your bank if financial payment has been taken or made and you believe it to be a scam.

Removing software:

Remote access tools like AnyDesk, TeamViewer, Quick Support, Zoho Assist and others are from genuine software companies, but they can be used with malicious intent.

It is important to uninstall anything that you don't recall downloading or that has appeared. If you do not feel capable of uninstalling remote software apps yourself, please speak to friends, family, or a local computer expert (please do your research first) to help you with this.

How to protect yourself

Data breach:

A data breach is a security incident where personal information, such as email addresses and passwords are breached/stolen from an organisation you may have been registered with.

For more information: www.ncsc.gov.uk/guidance/data-breaches.

- Visit: www.haveibeenpwned.com to check if your information has been compromised by a data breach. There is also a "Notify me" service available

- Change the password linked to the account involved in a breach using a secure password and enable 2-step verification on all online accounts (email, social media, online shopping)

If you think you might have been a victim of Cybercrime:

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

If you need more information with any online security, visit:

www.eastmidlandscybersecure.co.uk

www.ncsc.gov.uk/section/advice-guidance/you-your-family

Other frauds

Online shopping

Always be careful when shopping online, we receive a lot of reports whereby someone has purchased items via an online market place, the item is collected but upon checking the box it is often a different item or the box is empty. These are usually things like Apple products or gaming consoles.

Another one to beware of is car auctions, people will pay a deposit to secure the car, but the car is not actually for sale.

Be mindful when purchasing online, is the website legitimate? Take care of emails or online adverts with links with offers that sound too good to be true.

Pay with a credit card or other protected payment company such as Paypal. If it looks too good to be true it normally is.

Do your research into the item you want to buy and don't feel pressured into buying something.

Online jobs

The scheme looks very flexible and easy to work with, offering you the opportunity to choose when you work and enabling you to fit your work around your existing life, but may involve paying a fee to get you started.

The work itself could involve filling envelopes, assembling products or selling goods or services through your own website. In some cases, fraudsters may tell you there are faults with what you've done to avoid paying you. In other cases, the products you've bought or made are worthless.

Many of these business opportunities only allow you to earn money if you introduce more people to it. These are known as pyramid schemes.

Fraudsters may eventually sell your details on to others, so be alert to offers elsewhere.

Ticket fraud

- Only buy tickets from either the venue's box office, official promoter or agent, or a well-known ticketing website
- Avoid paying for tickets by bank transfer, especially if buying from someone unknown
- Be wary of unsolicited emails, texts or adverts offering unbelievably good deals on tickets

Is the vendor a member of STAR? If they are, the company has signed up to their strict governing standards. STAR also offers an approved Alternative Dispute Resolution service to help customers with outstanding complaints. For more information visit star.org.uk/buy_safe



Holidays

- **Check the travel company is legitimate.** About to book a holiday? Do some research first to check that the company is legitimate, especially if you haven't used them before. Use consumer websites, or reviews from people (or organisations) that you trust

- **Look for the logos.** Look for the ABTA, ABTOT or ATOL logos on the company's website. If you're unsure, you can use the links below to verify membership:

  ABTA - https://www.abta.com

  ABTOT - https://www.abtot.com/abtot-members-directory/

  ATOL - https://www.atol.org

- **Use a credit card to pay.** Use a credit card for payments (if you have one). Many of these protect online purchases as part of the Consumer Credit Act

- **Only provide required details at checkout.** When making your payment, only fill in the mandatory details (often marked with an asterisk) such as your address. Unless you think you'll become a regular customer, don't create an account for the store

- Watch out for suspicious links. Whether it's in an email or social media post, be wary of promotions for unbelievably good holiday offers. If you receive a suspicious email, report it by forwarding it to: report@phishing.gov.uk

Rental fraud

- Never send money to anyone advertising rental properties online until you are certain the advertiser is genuine, you or a reliable contact has visited the property with an agent or the landlord

- Ask for copies of tenancy agreements and safety certificates such as gas and electricity or a HMO licence

- Never be pressurised into transferring large sums of money. Transfer funds to a bank account having obtained the details by contacting the landlord or agent directly. Be sceptical if you are asked to transfer any money via a money transfer service like Western Union

Useful organisations

Report 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.reportfraud.police.uk

0300 123 2040

0300 123 2050

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

For our dedicated Scams Prevention and Support Service please telephone: 0115 855 3388 or email scamsawareness@ageuknotts.org.uk

Our main charity telephone line is open for information, signposting and advice 9am – 5pm Monday to Thursday and 9am – 4.30pm on a Friday. Alternatively email info@ageuknotts.org.uk

www.ageuknotts.org.uk

0115 844 0011

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

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

Nottinghamshire Victim CARE is a free, independent, and confidential support service for victims of crime, scams and fraud, commissioned by the OPCC.
Their caseworkers are here to listen and provide support on how to cope with difficult situations. Caseworkers are also trained to provide practical scam prevention information and advice or guidance on dealing with financial institutions and appeals to the Financial Ombudsman Service.

https://www.nottsvictimcare.org.uk/

0800 304 7575 or text NOTTSVC on 82228

support@nottsvictimcare.org

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

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

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 138 111

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

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

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

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/reportingscammail

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

www.royalmail.com

0800 0113466 (Message service only)

scam.mail@royalmail.com

Nottinghamshire County Council Trading Standards helps protect residents in Nottinghamshire against rogue traders and traders who have acted unfairly. Nottinghamshire County Council Trading Standards also provide support and advice to residents who have been the victim of a scam. To report a matter to Trading Standards and obtain advice, please contact the Citizens Advice Consumer Service.

www.citizensadvice.org.uk/consumer/get-more-help/if-you-need-more-help-about-a-consumer-isue/

0808 223 1133

Checklist

- [ ] **Change telephone numbers and make it ex-directory**

- [ ] **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

- [ ] **Call Blocker phones/Truecall:** A nuisance Call Blocker phone or a Truecall blocker can assist in blocking unwanted phone calls

- [ ] **Network Provider:** These can provide services to reduce unwanted calls (this is separate to the TPS service) and you can also try requesting limitation on international numbers if this facility isn't required

- [ ] **Mailing Preference Service (MPS):** Free register for individuals who do not want to receive unsolicited contacts by post
  Tel: 0845 703 4599 or visit: www.mpsonline.org.uk

- [ ] **Royal Mail:** Can report scam mail by posting directly to FREEPOST SCAM MAIL Tel: 0345 611 3413 or Email: scam.mail@royalmail.com

- [ ] **Contact your bank / credit card company:** If account details are compromised

- [ ] **CIFAS:** Is a non-profit membership association, a dedicated Fraud Prevention Service
  Call 0330 100 0180 to be added to CIFAS or visit http://www.cifas.org.uk

- [ ] **Check your full credit history,** you will be able to view is any other credit such as loans, mobile phone contracts etc have been taken out in your name. You need to register to view your full credit report – remember to cancel.

- [ ] **ID Material Compromised:**
  Passport: Passport photo or copy of passport sent – Tel: 0300 222 0000
  Driving licence: If this is compromised Tel 0300 790 6801 also contact your insurance company to advise should they be receive any claims of you crashing in to them.
  National Insurance number: Contact the Inland Revenue to confirm the compromise.
  Tel: 0300 200 3500 (Mon - Fri: 8am to 8pm & Sat: 8am to 4pm)

- [ ] **Remove yourself from the open register/Electoral Roll - OPEN REGISTER.**
  You are automatically enrolled upon voting, meaning anyone can request your & see your information, this can make you a target so contact your local council.

Notes

Notes

Notes



NOTTINGHAMSHIRE

POLICE

PROUD TO SERVE