Fraud prevention guide

Protect yourself against fraud and scams

We all think fraud and scams are something that happens to other people, until it happens to us.

We're working hard to protect you against fraud and scams, but there's lots of ways you can help protect yourself, too.

On this page, you can learn more about the different types of fraud and scams, and how to spot them.

Here's what to do if you're contacted unexpectedly by phone, email or text message:

1. Stop and think – if it's unexpected, be suspicious
2. Don't call numbers in messages or emails without checking they're genuine
3. Don't click on unfamiliar links - go to the official website or app
4. If in doubt, check with a friend or family member before taking action

What's the difference between fraud and a scam?

Fraud is a transaction, or suspicious activity on your account which you had no knowledge of and didn't authorise. A third party has performed an action on your account without you being aware.

A scam is where a criminal convinces you to reveal personal information or tell them your banking security details. They'll then attempt to convince you to knowingly authorise a payment from your account to a person, company, or for goods you believe to be genuine

How do scams or fraudulent activity happen?

Scammers usually contact people by email, text or phone. They often claim to be a person you would trust and try to get you to disclose personal details. They may say that they're from a bank, utility provider, HMRC or even the police.

Fraudsters can also communicate with you online. They may pretend to be your friend(s) or a member of your family, by hacking or spoofing their social media profiles and tricking you into sending them money.

They can sound genuine, as they may have gathered information about you online.

You can safeguard your personal details online, by checking your privacy settings and controlling what information you share.

To help keep your information secure:

- make sure your social media profiles are private
- destroy bank statements and similar documents safely
- always think carefully before sharing data with others
- stop and think before accepting a call, or responding to an SMS or email

Common methods fraudsters may use to contact you

Here are some common methods fraudsters will use to contact you:

Phone (vishing)

A common scam is when a criminal phones you out of the blue, claiming to be from your bank, the police, or another trusted organisation, like your broadband provider.

They can make the call seem authentic by using ‘number spoofing’. This is where they make their phone number look like a number you know and trust.

They may also have gathered some information about you, such as your address and account details.

The caller may try to persuade you to:

- transfer money to a 'safe account' or a known beneficiary, as your account is 'compromised'
- withdraw cash and hand it over to the 'police' for investigation
- press a number on your keypad to speak with a fraudster posing as a customer service representative
- give further personal and financial information

The caller may advise you to call the number on the back of your card if you tell them you think it’s a scam. Be aware that this can be part of the scam, as scammers can keep landlines open and play a fake dial code.

If you want to call your bank afterwards, make sure:

- you hang up the phone properly
- you wait 15 seconds
- the line is fully disconnected

- you wait another 15 seconds before beginning a new call, or use another device
- contact the organisation using a phone number you know is genuine

SMS (smishing)

Scammers often send fake text messages that look like they've come from your bank, or another trusted organisation. Their goal is to get you to reply with your personal or financial information.

Typically, they'll:

- encourage you to take urgent action by clicking on a link, or making a call
- ask you to verify new payees, transactions or devices
- try to look genuine by copying text messages sent by an organisation and adding their own wording
- often be sent from unknown mobile numbers

If you've received an SMS, you believe is suspicious:

- don't click on any links
- don't download any attachments
- don't reply
- delete the text message
- contact the organisation using a phone number you know is genuine, or visit their website

It's important to remember:

- banks and other organisations, such as the police, will never ask you for your full PIN, password, or banking codes
- we'll never text you a link that takes you directly to our online banking log on page

If you do click on a link, fraudsters may continue to contact you.

Email (phishing)

Phishing emails are unexpected messages that appear to come from a trusted organisation, such as your bank, HMRC, or a retailer you've purchased from.

Typically, they'll:

- encourage you to click on a website link
- urge you to take urgent action and threaten to close your account if you don’t respond
- say that you’re owed money
- ask you to give confidential or security information (such as your online banking details, passwords, account numbers or PINs)
- include instructions to reply, or verify your account – like completing a form attached to the email
- sometimes have poor spelling and grammar

If you receive an email you believe is suspicious:

- don’t click on any links
- don’t open any attachments
- don’t reply
- contact the organisation using a phone number you know is genuine, or visit their website

Common scams to be aware of

Authorised push payment (APP) scams
Authorised push payment (APP) scams happen when criminals persuade you to make a bank transfer. They often create a false sense of panic to make you send money before you have time to think it through properly.

Purchase scams
Purchase scams happen when you’re paying for an item, or service. The item doesn't arrive, or the service doesn't happen and your money is lost.

Typically, these scams:

- ask you to send money via bank transfer rather than using normal ways to pay
- seem too good to be true (because they probably are)
- have 'limited availability', or are a 'special offer' to encourage you to act quickly

- are typically advertised on social media or other online marketplaces, or in some cases through legitimate looking websites that have actually been setup by fraudsters
- persuade you to send money before receiving goods

Remember to:

- use safe sites when shopping online
- use safe ways to pay, such as your debit or credit card
- check the returns and cancellations policy
- research the retailer online to make sure they're legitimate
- stop and think - would you be willing to send cash in the post for an item you've ordered?
- research and check the validity of the item before agreeing to pay via other means
- If possible, ask to see the item before proceeding
- approach an independent professional to authenticate the goods or services you are purchasing

Investment scams

Criminals may contact you to offer investment opportunities which may seem too good to be true - offering guaranteed, or very high, returns.

They often cold call you, use false testimonials, fake celebrity endorsements, spoof websites and fake or cloned companies with similar names, or cloned names, to genuine investment organisations.

They can usually provide convincing marketing materials to make the scams appear genuine, or use current news and other media outlets to make the opportunity seem realistic.

Pension scams

Criminals claim they can unlock pension funds by moving them from an existing scheme to a new one, allowing early access to benefits before the legal age of 55. Victims may be instructed by the scammer to avoid telling their pension provider exactly why they're trying to withdraw funds.

Victims of these scams are usually asked to pay a very high fee and may also face serious tax consequences.

Be wary of scams like this and, if in doubt, seek advice from registered pension providers.

Remember to:

- check the Financial Services Register Financial Services Register This link will open in a new window on the FCA website to confirm the company is authorised, and to look for verified contact details
- verify that you're in contact with the genuine investment company. Visit the FCA websiteFCA website This link will open in a new window to check cloned firms and individuals
- visit the FCA Warning ListFCA Warning List This link will open in a new window to search for the firm or company you're dealing with
- conduct your research – if you're entering into a cryptocurrency investment, make sure you understand the offer and how the investment works
- contact the company on an independently verified number or email address and confirm that the person you're dealing with is a legitimate representative of their firm
- seek advice from a financial advisor

Payment diversion scams

Criminals can hack and monitor your emails, and when payments are due, they'll send their own email that looks and feels like a genuine message from a company, or firm.

They tell you that the bank details for your payment have changed, and give you the new details to send your payments to. This could be a house deposit to your solicitor, or a payment to a contractor for home improvements, for example.

Remember to:

- check with the company you're making a payment to, on a genuine phone number, before making a payment with new bank details
- check for poor spelling and grammar within the email – sometimes there can be errors which can be a strong indicator of a scam
- check the email address is correct

Romance scams

This type of fraud begins with a fast-moving, online relationship. Usually, a fake picture and profile are used.

To avoid meeting up in person, the fraudster may claim to be working overseas, for example, they may say they're in the armed forces, or working for a voluntary service.

Scammers try to lower your suspicions by appealing to your compassionate or romantic side, and then ask for money. They'll go to great lengths to build rapport and form a highly emotional bond.

To avoid falling victim to one of these scams, never send money to someone you've only met online. Don't agree to accept money from them to send on their behalf, as this could be the proceeds of crime.

Money mules
Criminals prey on those who are strapped for cash to act as 'money mules'. This means you agree to allow money to be transferred through your bank account in exchange for payment. Hard-up students are often targeted.

You'll be asked to provide your bank details, receive a payment into your account and then, either withdraw it in cash, or transfer it to another account.

Job adverts and spam emails offer 'easy money', and it might seem a harmless way to earn income. The money being transferred is stolen and used to fund organised crime.

This can get you into serious trouble. If you're caught, your bank accounts will be closed, you'll have problems applying for a loan, a mortgage or even a mobile phone contract. You may also be given a prison sentence of up to 14 years.

To learn more about the consequences of becoming a money mule and what the proceeds of money laundering are used for, check out the Don't Be Fooled websiteDon't Be Fooled website This link will open in a new window.

Holiday scams
There are many fake websites, online adverts, emails, social media posts and texts that promise great holidays or travel arrangements which are fake. Either the holiday doesn't exist – or it does exist, but has been sold to you by a criminal.

You might not realise you've been scammed until the flight tickets don't arrive, or you turn up at the resort, airport or cruise terminal only to find you've lost your money.

Where to find more information

Here are some useful links for the main UK organisations offering advice on how to guard against financial crime:

Action Fraud

You can report fraud or cybercrime to Action Fraud, a national reporting centre run by the City of London Police, working alongside the National Fraud Intelligence Bureau.

Cifas
This not-for-profit fraud prevention organisation was first launched in 1988 as the Credit Industry Fraud Avoidance System.

Cyber Aware
Previously known as Cyber Streetwise, this awareness campaign run by the Government, aims to help small businesses and individuals protect themselves against online criminals.

Get Safe Online
Get Safe Online offers free security advice to help protect people from fraud, abuse and other issues encountered online.

Financial Conduct Authority (FCA)
You can report scams to the FCA, an independent public body which regulates 58,000 businesses in the UK working in financial services.

Take Five
A government-backed national campaign led by Financial Fraud Action UK (part of UK Finance). Take Five offers advice on how to guard against financial fraud.