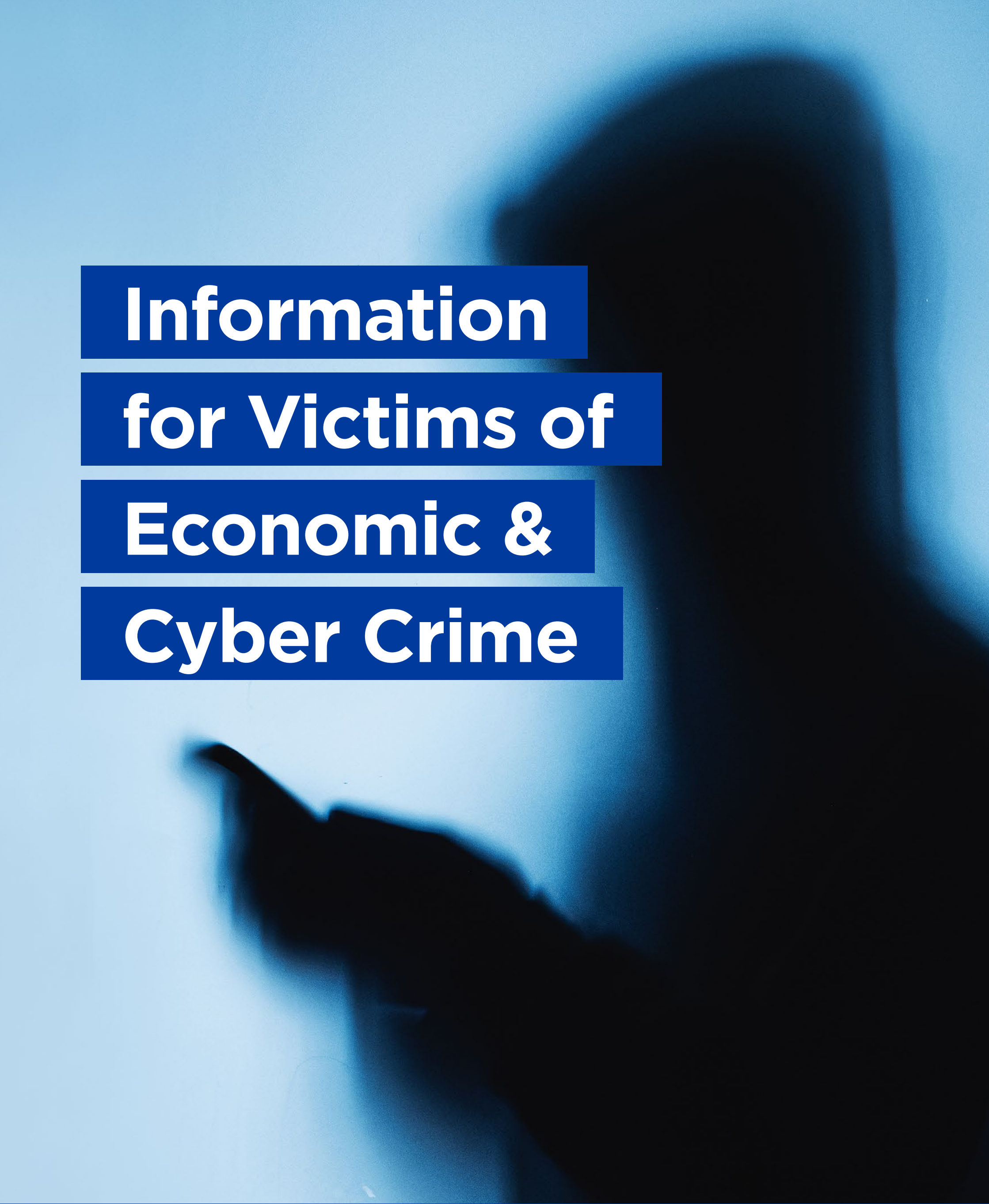


Information for Victims of Economic & Cyber Crime

METROPOLITAN POLICE

MORE TRUST | LESS CRIME | HIGH STANDARDS

Contents

Introduction

We are sorry to hear that you, or someone close to you, has been the victim of fraud or cybercrime. We understand that this may be an upsetting time.

This guide explains what to do and who can help. It gives clear steps, useful phone numbers and websites for support.

For videos and booklets about preventing common fraud and cybercrime offences, visit the Metropolitan Police website: https://www.met.police.uk/littlemedia/

What should I do first?

1. Make a report to Report Fraud
2. Inform your bank
3. Change your passwords
4. Enable two-step verification
5. Seek support from Victim Support

Reporting helps the police and other agencies understand these crimes and helps to prevent them.

It may stop other people from becoming a victim. You can report fraud and cybercrime even if no money was taken, including reporting suspicious emails, phone calls, text messages, social media or websites.

Report Fraud

Report Fraud is the national reporting centre for fraud and cybercrime in England, Wales and Northern Ireland.

You can report incidents **24 hours a day, 7 days a week** via https://www.reportfraud.police.uk/ or by phoning **0300 123 2040** between 8am - 8pm. Webchat is also available.

Within Scotland, fraud is reported directly to the police by calling 101.

Businesses, charities or other organisations suffering from a live cyber-attack should call 0300 123 2040 immediately. This service is available 24 hours a day, 7 days a week.

When you make a report, Report Fraud will give you a reference number. This begins ‘RF’. You can give this number to other companies when telling them what has happened.

Police

In most cases, the police will ask you to make a report to Report Fraud unless the crime is happening now, has just happened, or if the suspect is known and nearby.

If you feel in danger, call 999.

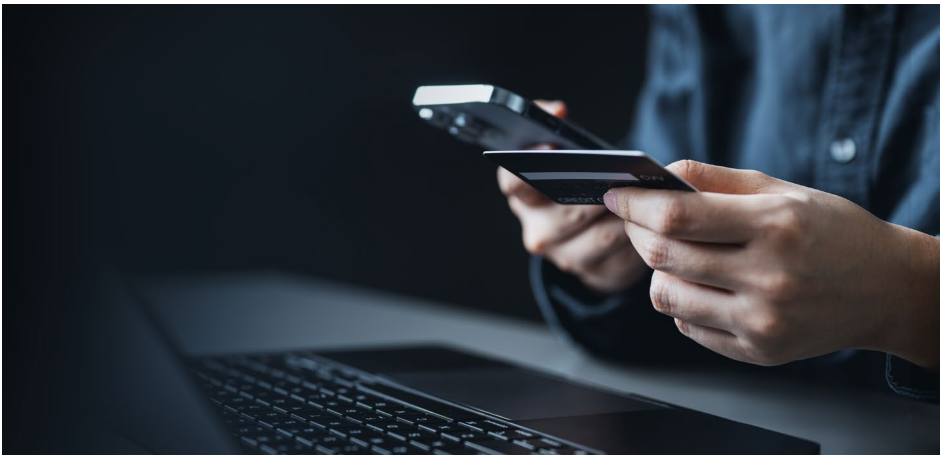
If you use textphone, call 18000. If you are registered for emergencySMS, you can text 999.

For non-emergencies, call 101 or use online contact methods.

Reporting to your bank

If money was taken from your account, tell your bank, payment company or exchange as soon as possible. They will act quickly to try to get the money back.

You can safely call your bank by dialling 159, or to check your bank's contact details, visit the Financial Conduct Authority's register; https://register.fca.org.uk/



Changing your passwords

Weak passwords are easier for criminals to crack. The longer and more unique your password is, the harder it is for criminals to get into your accounts.

One simple way of making this harder is to create a strong password by combining **three random words**. Avoid using common passwords like 'password' or personal details such as birthdays, anniversaries, favourite teams or pet names.

If you're thinking of swapping letters for numbers (such as changing 'o' to '0'), cybercriminals know these tricks too. It won't make your password much stronger – just harder for you to remember.

If you're worried about forgetting passwords, you can use a **password manager** which is like a secure digital folder that stores the passwords in one place. You only need to remember one strong password to access the password manager and it will then create passwords and save them for you. You can download a password manager application or use built-in options on your computer or web browser.

Enabling two-step verification

Many online services offer two-step verification (2SV), also known as two-factor authentication (2FA) or multi-factor authentication (MFA). **This provides an extra layer of protection to your accounts.**

When set up, you will be sent a PIN or code, often by text message or email. You then need to enter this number along with your password to prove it is really you.

You may also be able to add fingerprint authentication, face scan, use an authentication application or another method of verification.

Even if someone then knows your password, they cannot get into your accounts without the second step of security. Use two-step verification for your most important accounts such as email, banking, social media and online shopping.

The **National Cyber Security Centre** has advice on how to create strong passwords, turn on two-step verification, back up your data and install the latest software updates which can be found here: https://www.ncsc.gov.uk/collection/top-tips-for-staying-secure-online

Seek Support

Victim Support are a national charity that help people affected by crime. They offer free, confidential, practical help and emotional support across England and Wales.

Website: www.victimsupport.org.uk

Telephone: 0808 168 9111. Lines are open 24/7 every day of the year. They can also be contacted using the Relay UK app or using British Sign Language.

Live chat: victimsupport.org.uk/live-chat

My Support Space: mysupportspace.org.uk/MoJ

What happens after I’ve made a report?

When you make a report, this will be sent to Report Fraud Analysis Services. They will tell you what will happen within 28 days.

Report Fraud

Registering with Report Fraud will allow you to add information to your report, track progress on your report and call them to discuss your report.

If they think the case will be possible to investigate, **Report Fraud** will then send the case to the police force or agency best placed to do so. This might not be your local force. The local force or agency will also review your report and will tell you what may happen.

Not every report becomes an investigation but all reports are used to spot patterns of crime, take down fake websites or numbers, and warn the public about fraud and cybercrime.

If a police investigation is opened

If the police investigate your case, they will collect evidence and keep you updated on progress. Some investigations can take a long time to progress; especially when lots of banking or phone evidence is needed. Investigations aim to bring offenders to court.

Decisions on whether there is enough evidence to prosecute are made by the Crown Prosecution Service (CPS). If there isn't enough evidence, the case can't go ahead; no matter how serious the matter is or how much money has been lost. Hearings about getting money back are usually set after the case has been to court. Sometimes cases are dealt with in other ways than a prosecution.

Court cases

Information about what happens if a case goes to court is available via: https://www.met.police.uk/advice/advice-and-information/victim-support/going-to-court/how-courts-work/ along with what happens after you've given a statement to the police: https://assets.publishing.service.gov.uk/media/5a7aca88ed915d71db8b27ef/620956.pdf

If there is a court case, the defence can see copies of the documents created in the investigation. If you have given a statement, they will be given your name and you may be asked to give evidence at a trial. They will not be given your address, date of birth or contact details.

A Victim Personal Statement lets you tell the court how the crime has affected you (including feelings, health, money and safety). You can include concerns about if the defendant has been given bail, or if you believe you've been targeted because of who you are.

Knowing your rights as a witness or victim of crime

The Code of Practice for Victims of Crime explains the services you should get as a victim and how to complain if you are not treated properly.

For more information visit:
www.gov.uk/government/publications/the-code-of-practice-for-victims-of-crime

Compensation through the Criminal Courts

If someone is found guilty, the court may order them to pay compensation for some or all of the losses caused by the crime. The court decides on the amount of compensation. This depends on how much money the person has available to repay.

Civil Recovery of Funds

Money can also be seized by the police through civil proceedings. In most cases, civil recovery cases usually wait until after any criminal trial.

It may be possible for you to claim money through the civil courts. You may wish to get legal advice, speak to Citizens Advice (See page 19) or a Law Centre for advice on the best way to apply for compensation. The Financial Services Scheme (FSCS) may help in some cases (see '*my money has been taken*' on Page 31).

Reporting to other agencies

Reporting problems with investments, pensions or suspicious financial services

The **Financial Conduct Authority** regulate financial businesses in the UK. You can report problems with investments, pensions, loans, credit, insurance or suspicious financial services to them. They also have advice about your rights with banking, insurance, mortgages and financial advice.

Telephone: 0800 111 6768 (Freephone), 0300 500 8082 (from the UK) or +44 207 066 1000 (from abroad). They are open between Monday - Friday, 8am - 6pm and Saturday, 9am - 1pm

Contact form: https://www.fca.org.uk/contact#contact-form

Reporting suspicious HMRC emails, text messages and phone calls

His Majesty's Revenue and Customs (HMRC) are responsible for making sure the correct taxes are paid at the right time. They will never send notifications of a tax rebate or ask you to disclose personal or payment information by email or text message.

To report suspicious HMRC phone calls, use the **online form:** https://www.gov.uk/report-suspicious-emails-websites-phishing/report-scam-HMRC-messages-calls-social-media

Forward suspicious emails to HMRC's phishing team to phishing@hmrc.gov.uk

Forward suspicious text messages regarding the HMRC to 60599 (network charges apply)

Reporting of incidents which have happened via social media

In addition to Report Fraud you can report incidents directly to the social media company using their in-app tools on the platform:

Facebook: https://www.facebook.com/help

X (formerly Twitter): https://help.x.com/en

YouTube: https://support.google.com/youtube/

Instagram: https://help.instagram.com/

LinkedIn: https://www.linkedin.com/help/

Snapchat: https://help.snapchat.com/hc/en-gb

TikTok: https://support.tiktok.com

This helps the companies to identify and block suspicious profiles on their platforms.

Reporting of incidents which have happened via email

The **National Cyber Security Centre (NCSC)** (See page 36) is a government organisation that can investigate and take down fraudulent email addresses and websites.

Do not click on links in emails, open attachments or reply. If you have clicked on a link, do not provide any information on any sites that open.

You can mark email items as spam directly via your inbox.

Forward fraudulent emails to report@phishing.gov.uk

Reporting suspicious calls and texts

7726 spells 'spam' on the telephone keyboard. This will alert your service provider to investigate the number and potentially block it, if it's found to be a nuisance.

To report fraudulent calls, text the word 'call' to telephone number 7726 followed by the suspicious number.

Forward texts straight to 7726 followed by the suspicious number.

You can also report nuisance calls to **Information Commissioner's Office** (https://ico.org.uk/make-a-complaint/nuisance-calls-and-messages/spam-texts-and-nuisance-calls/) who collate information for potential enforcement action.

Reporting premium rate phone call fraud

Ofcom regulates services charged to phone bills. Report unexpected or high fees:

Telephone: 0300 123 3333 or 0207 981 3040

Online: https://www.ofcom.org.uk/make-a-complaint

Reporting fraudulent adverts

Report suspicious or misleading advertisements to the **Advertising Standards Authority (ASA)**. This includes any form of mass advertising, such as advertisements on television, radio, billboards, websites, and social media. The ASA can investigate and remove fraudulent adverts, as well as fine companies or individuals.

Website: https://www.asa.org.uk/make-a-complaint.html

Reporting fraudulent and junk postal mail

Report **fraudulent mail**, including fake lotteries or prize draws, to the Royal Mail at: https://www.royalmail.com/reportingscammail

Report **Royal Mail-branded suspicious emails, text messages, phone calls or websites** to reportascam@royalmail.com

Report **lost or stolen post** to the Royal Mail Security Team online. They have a help page available on their website: https://www.royalmail.com/report-a-crime

Further information about how to stop getting junk mail is available on the **Citizens Advice website:** https://www.citizensadvice.org.uk/consumer/post-and-parcels/stop-getting-junk-mail/

Reporting fraud offences where a company has been impersonated

If you've received a fraudulent email pretending to be from a company, tell the company directly. They can then warn their customers and take action.

Reporting businesses acting unfairly

Report businesses who break the law or act unfairly (including unsafe goods, fake items, items sold not as described, items not arriving, pressure selling, adding hidden costs or poor work quality) to **Trading Standards**. You can also tell Trading Standards if a business tries to stop you using your legal rights, such as saying you can't return faulty goods, or if they have sold restricted products to people underage.

To report to Trading Standards, contact the Citizens Advice consumer service.

Citizens Advice are a network of independent charities which offer free, confidential, impartial information and advice. They provide support on debt, money advice and consumer issues. Citizens Advice also operate the Witness Service in all Crown and Magistrates' Courts in England and Wales.

Your local Citizens Advice Service can be found on their website: https://www.citizensadvice.org.uk/about-us/contact-us/

Telephone:

England: 0800 144 8848, Wales: 0800 702 2020, Scotland: 0800 028 1456. This is available 9am - 5pm, Monday - Friday

Relay UK (if you can't hear or speak on the phone, type what you want to say): 18001. You can use Relay UK with an app or a textphone. There's no extra charge to use it.

Alternative methods of contact including accessible options are available on the Citizens Advice website: https://www.citizensadvice.org.uk/consumer/get-more-help/if-you-need-more-help-about-a-consumer-issue/

Reporting fraud against the NHS

The **NHS Counter Fraud Authority** investigates fraud, bribery and corruption in the NHS, as well as those who abuse their positions of trust; from patients and members of the public, to NHS staff, contractors, suppliers and organised crime groups.

Freephone: 0800 028 4060 (available 24/7)

Website: https://cfa.nhs.uk/

Online reporting form: https://reportfraud.cfa.nhs.uk/

Reporting serious bribery and corruption, or reporting as a whistleblower

The **Serious Fraud Office (SFO)** investigate serious or complex fraud, bribery and corruption. They cover England, Wales and Northern Ireland.

They take on a small number of large economic crime investigations which pose significant harm to people, industry or the economy of the UK and where cases need specialist skills to investigate.

For fraud offences, the SFO only accepts reports directly from corporate entities and whistleblowers. Members of the public should report fraud via Report Fraud (See page 5). If the report falls into the SFO's remit, it will be directed to them.

Website: https://sforeporting.egressforms.com/

Reporting anonymously

Crimestoppers is an independent charity which lets you report crime across the UK anonymously. Callers do not need to provide personal details, and calls cannot be traced.

Telephone: 0800 555 111 (24/7)

Website: https://crimestoppers-uk.org/

Rewards are sometimes offered and given without revealing the caller's identity.

My money or crypto has been taken

Contact your bank straight away. Fast action may stop the money being lost.

Inform the bank

If you can, tell the bank that received the money to stop it being sent on. You can find out which bank this was by using an online sort code checker.

Payment firms must follow reimbursement rules. This includes banks, building societies, smaller firms and e-money firms. In most cases, banks will reimburse innocent victims. Many people get money back (up to £85,000) within 5 business days.

Recovery fraud

Criminals sometimes contact you after a fraud, pretending to be the bank, police or recovery experts. They might say they have your money and need a fee or more details to give your money back. This is another common type of fraud. Criminals say this to get more information or money from you. If in doubt, contact the organisation using verified contact details to check what they're saying and that the person calling is employed by them.

To check a financial firm is authorised by the Financial Conduct Authority and their correct contact details, visit https://www.fca.org.uk/consumers/fca-firm-checker.

For transactions paid by Debit card

If you receive goods which are damaged, not as described or do not arrive, first try the seller's complaints process. If that fails, or they have gone out of business, ask your bank for a **'Chargeback'**. This process involves your bank getting the money back from where it had been transferred.

Chargeback can work for debit card and credit card purchases. It is not guaranteed and the rules are slightly different between card providers. You usually have 120 days from the transaction or expected delivery date to claim however in some cases this can be longer. If you're not sure, ask your bank. The seller can dispute this if they think it's an invalid claim.

There are examples available online for how to write a chargeback claim letter such as: https://www.which.co.uk/consumer-rights/letter/letter-to-make-a-chargeback-claim

For transactions paid by Credit card

Paying with credit cards gives stronger protection. For items costing between £100.01 and £30,000, the card company can be jointly responsible for the seller's breach of contract or misrepresentation. Claims for less than £100 may be possible, but this depends on your credit card provider.

Try to resolve disputes with the seller first, then contact your card provider. Aim to claim within 120 days of the transaction or expected delivery.

If you need to get new bank cards, set these up with extra security. Examples of this are Visa Secure, MasterCard SecureCode and American Express SafeKey.

Unauthorised Payments

Authorised Push Payments (APP) are when you are tricked into sending money to a criminal through a bank transfer. Regularly check your accounts for fraud, payments you don't recognise, or for too much money being taken out.

If this happens, contact your bank straight away and give them the details including the account where the money was sent. They will try to recover the funds.

For transactions made using crypto

Recovering crypto losses is usually harder than for other financial services. If you have had assets stolen from an exchange account, contact the exchange quickly and tell them what has happened. They might be able to flag the assets as stolen so that they can be frozen if possible. This needs to be done immediately as crypto can be moved very quickly.

Make a note of the transaction numbers for reporting and investigation.

There can be difficulty recovering crypto due to different legal frameworks with exchanges based abroad. Most crypto activity is not regulated by the Financial Conduct Authority (FCA) so the Financial Services Compensation Service will often not protect you if a crypto platform fails.

For information on securing your crypto, visit https://www.met.police.uk/SysSiteAssets/media/downloads/central/advice/fraud/met/little-book-crypto-crime.pdf

For transactions made via online marketplaces or via Online Payment Platforms

Buyer Protection may help if you paid but did not receive items purchased online. There are deadlines for making claims. More information can be found on the company websites.

If the payment was made via an online payment platform, check to see if you can make a claim under their dispute resolution process.

- **PayPal:** https://www.paypal.com/uk/cshelp/
- **eBay:** https://www.ebay.co.uk/help/
- **Facebook Marketplace:** https://www.facebook.com/help/
- **Gumtree:** https://help.gumtree.com/s/contact-us
- **Vinted:** https://www.vinted.co.uk/help

If a criminal uses a fake branded payment site page, the company themselves are not responsible for the transaction and you cannot claim a refund via Buyer Protection. You will need to report this to **Report Fraud:** https://www.reportfraud.police.uk/

Sellers can be victims of fraud too. **Seller Protection** may cover you but there are specific conditions and requirements which vary between companies.

For transactions made via Money Transfer Services

Payments sent via Money Transfer Services such as MoneyGram, PayPoint or Western Union are usually hard to get back. Each service gives advice on fraud prevention, so it's important to understand their guidelines before sending money.

For transactions made by cash, vouchers or gift cards

It is very hard to get money back if you paid with cash, vouchers or gift cards. Never share the numbers on the back of gift cards with anyone. Criminals pretend to be people you know or trust to encourage you to buy these for them. Verify what is being asked before purchasing.

I’m having problems getting my money back

If your bank refuses to refund you after a fraud but you believe you are entitled to one, there are steps to appeal.

Steps to appeal:

1. **File a formal complaint to your bank, card or payment provider.**

Initial reports of fraud should be filed with your bank as soon as possible, and within 13 months of the payment. You have the right to complain if you think your initial report was not handled properly. The payment provider has up to 8 weeks to reply. If they refuse to reimburse you, ask them to explain why.

If your bank details were used to set up a direct debit without your consent, the **Direct Debit Guarantee** protects you. Your bank should refund any unauthorised withdrawals, and you can complain if they don't.

If you did not keep your card, PIN or password safe, you may not be eligible for a full refund.

More information about the reimbursement protections for fraud victims can be found on the **Payment Systems Regulator (PSR) website:** https://www.psr.org.uk/information-for-consumers/app-fraud-reimbursement-protections/

If you were in a vulnerable situation at the time, tell your bank about this so that they can take it into consideration. **The Financial Conduct Authority's (FCA) guidance on the fair treatment of vulnerable customers** can be found here: https://www.fca.org.uk/publications/finalised-guidance/guidance-firms-fair-treatment-vulnerable-customers

2. Contact the Financial Ombudsman Service (FOS)

The Financial Ombudsman Service help settle disputes between you and financial companies. They are free, fair and impartial and listen to what you, the bank, and other people have said. They may ask for more information about what has happened to make a decision.

You must complain to the FOS within 6 months of getting a final response to your bank complaint or from the end of the 8 weeks if they haven't responded. Include any evidence in your complaint including what you want to happen.

Telephone: 0300 123 9123

Online: https://www.financial-ombudsman.org.uk/contact-us

3. Contact Citizens Advice (See page 19)

4. Make a court claim or resolve through mediation

You can apply to a county court to claim money you're owed by a person or a business. This used to be known as taking someone to a 'small claims court'. You can apply online or by post.

Information about how to do this is available on the government website: https://www.gov.uk/make-court-claim-for-money

5. Using a Financial Advisor or Claims Management Company

Financial advisors or companies can help by guiding you through the process, checking if you're eligible for compensation, and handling the paperwork or negotiations on your behalf. Choose a company or individual who is regulated by the Financial Conduct Authority.

Information on who is registered can be found on their website: https://www.fca.org.uk/firms/financial-services-register

It is also possible to **check whether an individual or company is already known to the FCA for being unregulated or unauthorised:** https://www.fca.org.uk/consumers/warning-list-unauthorised-firms

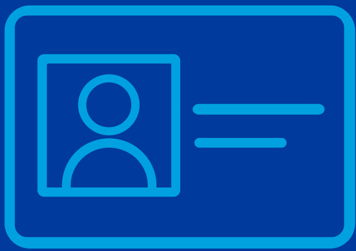
Just because someone isn't listed as unauthorised, they may not necessarily be legitimate. Be wary of recovery fraud (See page 23) if a company says they can get money back for you.

6. Apply for the Financial Services Compensation Scheme (FSCS)

The Financial Services Compensation Scheme (FSCS) pays compensation when authorised financial firms fail or cannot meet claims. This is an independent, government-established body and is free to use.

Telephone: 0800 678 1100 or 020 7741 4100

Website: https://www.fscs.org.uk/



My personal data or identity was stolen

Even when we protect our information, data breaches can still happen which make us vulnerable to identity theft and fraud.

What is a data breach?

A data breach is when someone gets your information without permission. Criminals use data breaches to commit fraud; sometimes to target you and sometimes pretending to be you. They may pretend to be from legitimate companies to persuade you to click on links in messages and emails; even if your data wasn't stolen.

If you think your data has been taken:

1. **Check if your email address has been involved in a data breach** by visiting https://haveibeenpwned.com. Similar services are often included in antivirus or password manager tools you may already be using. If you do find your email address has featured in a breach, change the password to that account and all other accounts where the same password has been used (See page 7).

   If you receive a message or email containing one of your passwords, don't panic. If it's a password you still use, change it as soon as you can. If any of your other accounts use the same password, you should change them too.

2. **Log out of all devices and apps -** After changing your passwords, sign out of your applications so anyone trying to use your account with your old log-in details must enter the new password.

3. **Monitor your accounts and credit reports** for any unusual activity. Tell your bank or account provider if you notice any activity, transactions or credit applications you haven't made.

   If you notice that a company is using your personal details without your permission, such as your name or address, **inform Companies House** by filing a form online: https://www.gov.uk/guidance/report-a-company-using-your-personal-details-without-your-permission

4. **Watch out for fake messages**. These may look official, offer password resets or compensation. **Check with the organisation** if this is real by using their official website or social media channels. Do not click on links you've been sent in emails or text messages. Guidance on spotting these messages and calls is available on the **National Cyber Security Centre's website:** https://www.ncsc.gov.uk/collection/phishing-scams/spot-scams

5. **Report lost or stolen documents** (e.g. passport, driving license, cards, cheque books) to the issuer and the police.

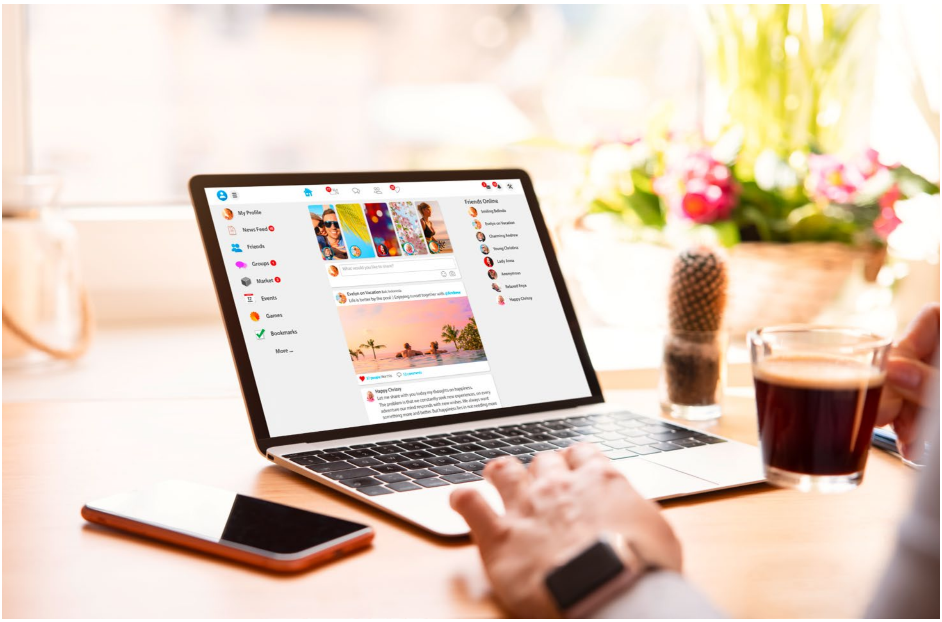
6. **Consider Protective Registration** (See page 60).

Social media impersonation

If you think your social media account has been copied, **report the fake account directly using the platform's reporting tools.** Reports usually need to come from the person being impersonated or their parent or guardian. Ask the person to report it themselves if possible.

Search for your name including any nicknames or previous names, online. If you find harmful or fake content, take a screenshot and ask the site to remove it using their 'Contact Us' information. You may also need to ask the search engine to remove results.

Check your privacy settings on social media, restrict access to only people you know and avoid oversharing information (for example, do not post personal information which is often used in security questions, such as favourite pets or schools attended).



Further information:

National Cyber Security Centre

For more guidance on data breaches, visit: https://www.ncsc.gov.uk/guidance/data-breaches

For guidance on how to use social media safely, visit: https://www.ncsc.gov.uk/guidance/social-media-how-to-use-it-safely

National Protective Security Authority

Learn about digital footprints and how what is posted or done online can make you or your organisation a target for criminals: https://www.npsa.gov.uk/security-campaigns/my-digital-footprint

The Cyber Helpline

The Cyber Helpline provide free, expert help for victims of cybercrime and online fraud. They have a 24/7 helpline for people over 13 years old, and sole traders.

Website: https://www.thecyberhelpline.com/gethelp

UK - Safer Internet Centre

The UKSIC work to identify threats online and provide advice to keep people safe, including help reporting impersonation on social media.

Website: https://saferinternet.org.uk/

Mail Preference Service

The Mail Preference Service is a free service supported by the Royal Mail which allows UK customers to take their name and home address off mailing lists to reduce the amount of marketing they receive.

Website: https://www.mpsonline.org.uk//

Telephone: 020 7291 3300

You can also pay to redirect your mail if you move home: https://www.royalmail.com/personal/receiving-mail/redirection

Voters Register

When you register to vote, opt out of the open register to reduce junk mail. This does not affect credit checks.

Website: https://www.gov.uk/electoral-register/opt-out-of-the-open-register

Register your land

Register your property with the Land Registry and keep your details up to date. Set alerts and add restrictions for changing records, such as needing a solicitor to verify any amendments.

Website: https://landregistry.uk/

Guidance on how to set up a Property Alert:
https://propertyalert.landregistry.gov.uk/

I’m still being contacted

Criminals will keep contacting you trying to get more money. They sometimes pass your details on to other criminals to target you again. There are ways to stop this.

If you receive ongoing contact:

Contact your phone provider

Ask what call blocking solutions they may have (for example BT Call Protect, EE Call Protect, or Sky Talk Shield) and ask them to make your phone number unlisted (ex-directory). This will stop your phone number from appearing in phone books and online directories.

Register with the Telephone Preference Service

The **Telephone Preference Service (TPS)** is the UK's official 'Do not call' register for landline and mobile numbers. It is free to register and lets people opt out of unwanted live sales and marketing calls. Organisations must not call a registered phone number after it has been registered for 28 days.

Website: https://www.tpsonline.org.uk/register

Telephone: 0207 291 3320

Check the IP address

An IP address is a unique number that identifies a device on a network and shows it's approximate location.

Public information is available via companies such as Scamalytics, who provide a lookup service for IP addresses. Their lookup allows anyone to view if an IP address is likely to be associated to fraud. For example, if a transaction claims to be from London but the IP address is in another country, this is a warning sign for fraud. Similarly, lots of accounts being created from the same IP address can be a warning sign of organised fraud.

Website: https://scamalytics.com/ip

Block unwanted contact

Block numbers by reporting them as spam or blocking them from your handset. Your phone manufacturer or service provider will be able to advise how to do this on your device. Advice on how to report spam messages and calls is on page 17.

Block contacts or messages by reporting the profiles to the platform directly.

If calls or messages carry on, obtain or install a call blocker. These can be physical devices which are plugged into your phone line or can be smartphone applications. These filter the incoming calls to your device.

Change your phone number if the contact continues, to avoid unwanted contact.

For in-person targeting

- Install a 'no cold calling' sign at your address. If people still knock, then you should not engage with them.
- Discuss with a neighbour if they are able to help you if people come to your door.
- Install a video doorbell or a CCTV camera with a warning sign.
- Register with the Priority Services Register. This allows you to set up a password for when electricity or gas company employees call you or knock at your door.

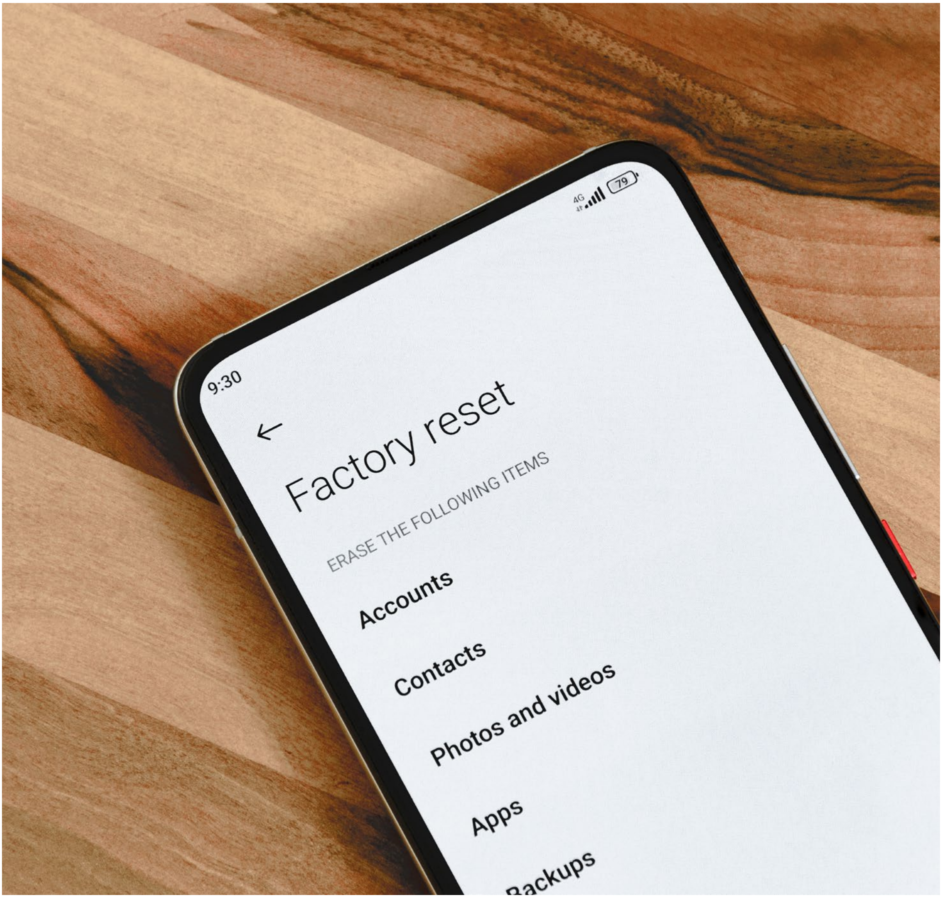
Website: https://www.thepsr.co.uk/

My device or account has been hacked

If you are concerned that your device or one of your accounts has been infected with a virus or accessed without your consent, take action immediately to restore access.

Signs you may have been hacked:

- You cannot log in to your accounts
- Security settings have been changed
- There are messages you did not send
- There are logins from places or times you do not know
- Unknown payments or transfers have been made



Confirm your device is infected with a virus

This may be through your antivirus protection saying that the device is infected, or the display shows ransomware asking for money. **Run an antivirus scan to check**.

If you're not sure, look for signs such as the device running slowly, restarting on its own or closing or opening applications unexpectedly. There might be pop-ups from unknown programs asking you to do things, or your friends may tell you about odd emails from you. On mobile phones, there could be warnings being displayed about jailbroken devices.

Try & fix it yourself:

- On phones or tablets, carry out a factory reset. The guidance on how to do this will vary between devices so check your manufacturer's guide.
- On laptops or computers, run antivirus products. If your antivirus can't clean the device, you will need to wipe the device entirely and reinstall everything. If you can't download and install an antivirus product, you will need to get expert help.
- Restore your backed up data from the last known backup which didn't have a virus on it. You may lose some recent data, but this prevents you from reinfecting the device from a later backup.

If this is unsuccessful, **get expert help**.

After you’ve fixed the infection

Make sure the device is set up securely; **install security updates regularly and back up your data**.

Guidance on how to do this is available on the National Cyber Security Centre’s website; https://www.ncsc.gov.uk/guidance/hacked-device-action-to-take

Inform the account provider

Visit the company’s help pages to report that your account has been accessed without your consent and follow their account recovery process. If you can’t get into your account, you may need to create a new one. When this is set up, tell your contacts that you’re not using your old one. Update banks, shops and services with your new account details.

Notify your contacts

Tell friends and contacts that your account was hacked or that you’d had a virus so they do not trust any strange messages sent from your account.

Check Your Email Account

Look for email forwarding rules and filters that send copies of your emails elsewhere. Remove any you did not set up. Instructions on how to do this will be on your provider's website.

For help on recovering hacked accounts, visit the National Cyber Security Centre's website: https://www.ncsc.gov.uk/guidance/recovering-a-hacked-account

Update your devices

Regularly install updates for apps and software and turn on automatic updates as these often include important security updates. Updating might take some time, so do this while connected to WiFi and while your device is charging if possible.

I'm struggling financially as a result

If fraud or cybercrime has left you in debt or struggling to pay your bills, the following organisations are able to provide advice.

Citizens Advice

(See page 19) for details.

Department for Work and Pensions (DWP)

The Department for Work and Pensions are responsible for welfare, pensions and child maintenance. They provide the State Pension and a range of working age, disability and ill health benefits. You can check the benefits and financial support you may have access to.

Website: https://www.gov.uk/browse/benefits

Directgov

Directgov provides easy access to public services and information. For help with understanding the benefits system and to talk through your entitlements, contact Jobcentre Plus.

Website: www.direct.gov.uk (Money, Tax and Benefits section)

Telephone: 0800 055 6688

To find contact details to search for a **lost pension** visit: https://www.gov.uk/find-pension-contact-details. You need to know the name of the employer or pension provider to use this service.

MoneyHelper

MoneyHelper is a free service provided by the Money and Pensions Service; sponsored by the Department of Work and Pensions. It offers free and impartial money and pension's guidance.

Website: https://www.moneyhelper.org.uk/

Telephone: 0800 138 7777 (English) or 0800 138 0555 (Welsh)

Typetalk: 18001 0800 915 4622

WhatsApp: +44 77 0134 2744

Webform: https://www.moneyhelper.org.uk/en/contact-us/money-guidance/money-guidance-enquiry-form

Civil Legal Advice

You may qualify for free, confidential advice from Civil Legal Advice (CLA) which is part of Legal Aid if you're in England or Wales. If eligible, you can get help for debt and help if your home is at risk amongst other problems.

You will need to provide proof of your finances and, if eligible, you will be able to contact a legal advisor who will decide what advice you can get. You can also ask CLA to call you back if you do not want to pay for the call by texting 'legalaid' and your name to 80010. There is a free interpreting service and you can also book a British Sign Language Interpreter.

To check eligibility, visit https://www.gov.uk/legal-aid/check-legal-aid

Telephone: 0345 345 4345

Minicom: 0345 609 6677

National Debtline

National Debtline are a charity run by the Money Advice Trust, who provide free, impartial and expert advice to help people deal with their debts.

Telephone: 0808 808 4000
(Monday - Friday, 9am - 8pm, Saturday, 9:30am - 1pm)

Website: https://www.nationaldebtline.org/

StepChange Debt Charity

StepChange provide free, confidential, 24/7 debt advice regardless of the size of your debt and can give you a tailored action plan to help manage it. They can help you plan to repay what you owe at a rate you can afford.

Website: https://www.stepchange.org/

Telephone: 0800 138 1111 (Monday - Friday, 8am - 8pm, Saturday, 9am - 2pm)

They also provide advice through British Sign Language interpreters.

Turn2Us

Turn2Us is a national charity providing help to people who are struggling financially. Their website has information about what support you can get and includes a benefits calculator as well as information about grants. The **'Find an Advisor'** tool allows you to look for local, regional or national organisations who can help you including information on benefits, housing, legal issues and mental health.

Website: https://www.turn2us.org.uk/get-support

Community Money Advice

Community Money Advice are a charity which supports community groups and churches set up free, face-to-face debt and money advice services locally.

They have self-help guides and budgeting advice on their website as well as free, confidential advice in person in England and Wales. If you are not near a centre, you can get help from a ChatBot who can put you in touch with an advisor.

Website: https://www.communitymoneyadvice.com/

Telephone: 01743 341929

Email: info@communitymoneyadvice.com

My mental health has been impacted

It is common for people to feel stress, anxiety or shame. Remember - this was not your fault.

Criminals use clever ways to deceive you into sending money or personal information. You are not alone. This was not your fault.

Tell your bank or loan provider if your mental health is affected so that they can help you. They may be able to add a note about your health to your file.

You can add a note to your credit file yourself through a **'notice of correction'** (See page 61). This may slow down applications for credit if you are worried about increasing your loans. You can also ask them to send a **'Debt and Mental Health Evidence Form'** to your doctor.

The following agencies can help you if your mental health has been impacted:

NHS

If you or someone else is having a medical emergency, call **999** or go to your nearest Accident and Emergency department (A&E).

For non-emergency help, call NHS Direct on **111** or visit NHS 111 online. This is a confidential helpline, available 24 hours a day.

The **NHS Better Health Every Mind Matters** website gives tips, self-help plans and ways to help others with mental health challenges.

Website: https://www.nhs.uk/every-mind-matters/

Debt Respite Scheme (Breathing Space)

If you are struggling with debt, you can apply to join the Debt Respite Scheme. This gives you legal protections if you are in debt.

'Standard' Breathing Space is available to anyone with problem debt and prevents creditor action for up to 60 days.

'Mental Health Crisis' Breathing Space is available to anyone receiving mental health crisis treatment and has stronger protections. An Approved Mental Health Professional must apply on your behalf. This lasts as long as the mental health crisis treatment, plus a further 30 days.

Website: https://www.gov.uk/government/publications/debt-respite-scheme-breathing-space-guidance/debt-respite-scheme-breathing-space-guidance-for-creditors

Mental Health & Money Advice

Mental Health & Money Advice is a UK-wide online advice service which helps you understand, manage and improve your financial and mental health. They provide support for both mental health and financial problems and understand that together these can create more problems.

Website: https://www.mentalhealthandmoneyadvice.org/en/help-contacts/

Samaritans

The Samaritans are a 24/7 support service for people who need support to prevent crises; in particular those contemplating suicide. Their contact number works from mobiles without credit and does not show up on phone bills. Details of your nearest branch can be found on their website.

Website: https://www.samaritans.org/

Telephone: 116 123

Email: jo@samaritans.org (it may take several days for them to respond to emails)

Face to face: https://www.samaritans.org/branches/

Mind

Mind are a mental health charity across England and Wales who provide information, advice and local services. They help people understand their mental health and what help is available through a confidential information line, a legal line, and information online and in print. They provide online peer support, treatment options, advocacy services, welfare benefits information and information about local support.

Website: https://www.mind.org.uk/

Telephone: 0300 123 3393, Monday - Friday, 9am - 6pm

Email: info@mind.org.uk

Hub of Hope

The Hub of Hope is a mental health support database provided by charity Chasing the Stigma which brings local, national, peer, community, charity, private and NHS mental health support services together. They signpost people in times of crisis and when you need extra support. They also provide support for family members and friends.

Website: https://hubofhope.co.uk/

British Association for Counselling and Psychotherapy

The British Association for Counselling and Psychotherapy give free information on counselling services in your area and a list of counsellors available.

Website: www.bacp.co.uk

Telephone: 91455 883 316 (Counselling services) or 01455 883 300 (General Enquiries)

Rethink

Rethink Mental Health aim to give support, advice and information about mental health and have information about services in your local area.

Website: https://www.rethink.org/

Counselling Directory

The counselling directory gives information about counselling as well as listing counsellors across the UK with their contact details, fees and the areas they cover. The Directory is free, confidential and easy to use. They also have advice, self-help articles and a podcast.

Website: https://www.counselling-directory.org.uk/

Asian Family Counselling Service (AFCS)

The Asian Family Counselling Service offers confidential counselling service to members of the Asian community in Urdu, Hindi, Gujarati, Punjabi and English. You can contact them directly or referrals can be made by doctors, social workers, solicitors or other health professionals.

Website: https://asianfamilycounselling.org/

Telephone: 0208 571 3933 or 0208 813 9714

Email: afcs@btconnect.com

Muslim Community Helpline

The Muslim Community Helpline provide emotional support and counselling, referrals and practical help to members of the Muslim community.

Website: www.muslimcommunityhelpline.org.uk

Telephone: 0208 904 8193 or 0208 908 6715 (Lines open Monday - Thursday, 10am - 1pm and Friday, 10am - 4pm)

Email: ee4m@btinternet.com

JAMI (Jewish Association for Mental Illness)

JAMI is a mental health service for the Jewish community. They give support and advice for adults, young people and their families or carers. They offer peer support both online and in-person with community hubs in Hackney, Redbridge and Finchley.

Website: www.jamiuk.org

Telephone: 020 8458 2223, Monday - Friday, 9am - 5pm

Email: info@jamiuk.org

The Salvation Army

The Salvation Army is a Christian charity across the UK & Ireland which has 650 churches and community centres where they offer friendship, practical help and support to disadvantaged people including debt advice.

Website: www.salvationarmy.org.uk

Telephone: 0207 367 4500

Childline

Childline provide a free, private and confidential 24/7 helpline to anyone under the age of 19 in the UK. They have trained counsellors to support you.

Website: https://www.childline.org.uk/

Telephone: 0800 1111

1-2-1 Counsellor Chat: https://www.childline.org.uk/get-support/1-2-1-counsellor-chat/

My credit has been impacted

If a criminal takes out a loan or borrows money in your name, your credit score could be harmed. There are things that you can do.

What is credit?

Credit is borrowing money from a lender and then paying it back. Credit ratings are how likely you are to repay anything you borrow, based on your history of managing your money. The rating helps lenders decide whether they should give you a loan, insurance, or rental agreements.

If a criminal takes out a loan or borrows money in your name, your credit score could be harmed.

A few companies, including Experian, TransUnion, Crediva and Equifax, offer free credit score checks.

Regularly reviewing your score helps to spot anything you don't recognise. Some paid-for services send alerts or let you lock reports. Report unknown accounts or loans to the bank or firm at once.

What is a Cifas warning?

Cifas is a not-for-profit organisation that helps stop financial crime. They work with various organisations to protect their customers and the public.

Their warning list lets lenders put markers on your credit file if they suspect fraud. Lenders are legally required to report these concerns.

If you see **'Victim of Impersonation'** written on your credit report and you weren't told about it, do not panic. It means that an organisation has flagged your file due to suspected fraud.

If you haven't heard from the organisation that put the marker on after a week, contact them to get more information - their details will be on your report. This warns other organisations to complete extra checks if loans are taken out or new accounts opened in your name. These warnings last on your file for 13 months. They do not impact your credit score or prevent you from applying for loans or credit in the future.

Website: www.cifas.org.uk

Protective Registration

If you've been a victim of fraud, you can apply for the Cifas Protective Registration Service which costs £30 for two years. This adds a warning flag to your details, alerting lenders that you may be at risk of fraud. It ensures that additional checks are performed when looking at credit applications in your name.

You can access this service at https://www.cifas.org.uk/pr and requires filling in a form.

How do I dispute something in my credit report?

If you identify any mistakes, report them to the filing organisation who have 28 days to respond. Your problem will be marked as ‘disputed’ on your file while they check.

If possible, contact the credit agency so that they can update the record. They can update or remove information on your report if the company confirms it is incorrect.

What is a Notice of Correction?

If you find anything on your credit report that you think needs more information, for example, that you were a victim of fraud, you can ask credit agencies to add up to 200 words to your file as a Notice of Correction.

Lenders should read this when they check your report before reviewing any applications.

Check your report at least once a year to make sure it’s right. If you have been the victim of identity theft, check it more often.

Adding a Password to Your Credit Report

You can add a password to your credit report so that lenders need to ask for it before allowing new credit applications in your name. This process varies depending on the credit report provider.

My business's data has been stolen

If you believe that your company has been the victim of a cybercrime or fraud, there are certain steps you will need to follow.

You may need to tell different organisations. If unsure, **use the Cyber Incident Signposting Service (CISS) for help** - https://www.gov.uk/guidance/where-to-report-a-cyber-incident

1. **Report** - By law, you need to report a personal data breach to the **Information Commissioner's Office** without delay and within 72 hours. If the breach is reportable, submit it online. The ICO offer a self-assessment tool to help you decide: https://ico.org.uk/for-organisations/advice-for-small-organisations/72-hours-how-to-respond-to-a-personal-data-breach/

2. **Don't panic** - not every breach reported to the Information Commissioner's Office results in formal action. They aim to help organisations avoid something similar happening in the future.

3. **Find out what happened** - make a timeline of what you know and actions you've taken so far.

4. **Try to contain the breach** - if you can recover the data, do so immediately.

5. **Assess risks to the people affected** (for example, safeguarding, identity theft or distress) and give clear advice on what they can do to protect themselves.

National Cyber Security Centre (NCSC)

The National Cyber Security Centre (NCSC) is a part of GCHQ and is the UK's leading authority on cyber security. It helps public bodies, industry, small and medium sized enterprises, and the public. When cyber incidents occur, they respond, give guidance and help the UK stay safe online.

Website: https://www.ncsc.gov.uk/

To **report cyber incidents** to them, visit https://report.ncsc.gov.uk/

Business Debtline

Business Debtline is a UK-based charity offering free, impartial and expert advice to self-employed people and small businesses facing financial challenges. Their advisers give debt advice and support. They also have a webchat function and an online budget calculator which you can use before calling.

Website: https://mybudget.businessdebtline.org/

Telephone: 0800 197 6026 (Monday - Friday, 9am - 8pm)

Cyber Protect

The Metropolitan Police Cyber Protect team help small to medium sized businesses and charities. They offer advice, presentations and planning exercises to raise awareness of cyber threats and help organisations protect themselves. Their services include:

- Cyber awareness presentations
- Scanning online systems for vulnerabilities
- A Decisions and Disruptions exercise
- A cyber escape room
- NCSC Exercise in a box

Website: https://www.met.police.uk/cyberprotect

I want to support someone else

Fraud can significantly impact people’s lives. It’s not just a loss of money but is also a loss of trust and confidence. Victims also need to work out the legal processes and how to recover funds.

Office of the Public Guardian

The Office of the Public Guardian is responsible for protecting people who no longer have the capacity to make certain decisions for themselves.

Lasting Power of Attorney (LPA) must be created when a person is mentally capable of understanding what they are doing. It can be done by anyone over 18; you don't need to be unwell and it covers issues of finance and property.

If someone is unable to look after their affairs but hasn't drawn up a Power of Attorney before losing capacity, you need a court to authorise you to make decisions about their finances. The **Court of Protection** appoints a deputy who is usually a family member or a close friend.

Website: https://www.gov.uk/government/organisations/office-of-the-public-guardian

My Support Space

My Support Space is an online tool from Victim Support to help people after they've been a victim of crime. It offers guides you can work through at your own pace.

They also provide a range of coping strategies for feelings of avoidance, denial, compulsive behaviours and physical behaviours linked to fraud.

Website: https://www.mysupportspace.org.uk/

Redirecting mail on behalf of someone else

You can apply to redirect mail on behalf of someone who has died, or for whom you have Power of Attorney, via an application form.

Website: https://www.royalmail.com/personal/receiving-mail/redirection

Every Mind Matters

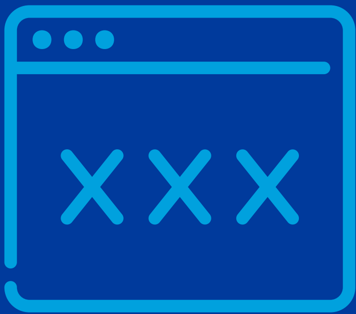
The National Health Service (NHS) provide information on how to support other people with their mental health. Their website gives information about what you can do when someone needs more help.

Website: https://www.nhs.uk/every-mind-matters/supporting-others/helping-others/

Childnet

Childnet are a charity who help children, young people, and their supporters to stay safe online.

Website: https://www.childnet.com/



Illicit content has been shared about me online

Stay calm: non-judgemental help is available.

1. **Do not pay demands for money**
2. **Keep evidence**
3. **Change your passwords for any compromised accounts**
4. **Report to the platform**
5. **Report to Police**

Sexually motivated extortion ('sextortion') is when criminals threaten to share private images or videos unless you pay them. They sometimes have access to these images but sometimes they only say they do to scare you. They may provide your passwords or account information to make the threat seem real. If this happens:

- **Stay Calm.** Remember; non-judgemental help is available.
- **Do not pay.** Paying often leads to more demands and doesn't mean the criminals won't send the images anyway. If you've already paid, keep proof and try to cancel the payment.
- **Keep Evidence.** Take screenshots of all messages, images and links. Record all details such as the criminal's social media profile URL and ID numbers (rather than just usernames, as these can be easily changed), phone numbers and payment details. After doing this, block all contact.
- **Change your passwords to any compromised accounts.** (See page 7).
- **Report to the social media platforms.** Make profiles and friend lists private and do not accept contact from new profiles you don't recognise in case this is also the criminal. Ask the social media platform for removal of the images.
- **Report to the police.**

Report Harmful Content

Report Harmful Content can help you report different types of harmful content online. Before reporting to them, you need to have reported the material to the social media service directly at least 48 hours beforehand. Information on how to do this is on their website. They can accept reports from people aged 13 or over.

Website: https://reportharmfulcontent.com/

Revenge Porn Helpline

The Revenge Porn Helpline gives confidential support to people whose intimate images have been shared without consent. They can also provide guidance on how to remove intimate content.

Telephone: 0345 6000 459

Email: help@revengepornhelpline.org.uk

Website: https://revengepornhelpline.org.uk/

Stop Non-Consensual Intimate Image Abuse is run by the Revenge Porn Helpline and is a free tool to support victims of non-consensual intimate image abuse. It helps create a digital fingerprint of your images so participating companies can block them from being shared. It uses data directly from your device so does not download the image, and collects minimal data.

Website: https://stopncii.org/

Thinkuknow

The Child Exploitation and Online Protection (CEOP) Safety Centre, run by the National Crime Agency, aims to help protect children and young people from online abuse. They do this through training professionals, young people and their families.

Online reporting programme: https://www.ceop.police.uk/ceop-reporting/

Childline

Childline provide free, private and confidential 24/7 help and counselling to anyone under the age of 19 in the UK.

The **Report Remove** system helps children confidentially report and remove sexual images and videos of themselves from the internet. Reporting refers the case to the Internet Watch Foundation (IWF) and they can also put you in touch with a counsellor for any extra support.

Telephone: 0800 1111

1-2-1 Counsellor Chat: https://www.childline.org.uk/get-support/1-2-1-counsellor-chat/

Website: https://www.childline.org.uk/

Report Remove: https://www.childline.org.uk/info-advice/bullying-abuse-safety/online-mobile-safety/report-remove/

Preventing further offences

Lots of the organisations featured in this booklet publish information about how to protect yourself from fraud and cybercrime.

The Metropolitan Police have created a series of booklets, videos and guides, which are available in accessible formats, to raise awareness of common fraud and cybercrimes methods and how to stay safe. These can be found on our website https://www.met.police.uk/littlemedia

Stop Think Fraud

Stop Think Fraud is the national campaign against fraud created by the UK Government. Their website gives information and advice about protecting yourself and others from fraud, and how to recover after being a victim.

Website: https://stopthinkfraud.campaign.gov.uk/recovery-from-fraud/

UK Finance

UK Finance is the trade association for the finance industry in the UK. Their website has information on how you can protect yourself and your business from fraud and cybercrime.

Website: www.UKFinance.org.uk

Other support available

Bank Safe Online

Bank Safe Online is run by the Payments Council and aims to provide advice and tips on how to use online banking services securely and with confidence.

Website: http://www.banksafeonline.org.uk/

Get Safe Online

Get Safe Online is a UK based internet safety website. They provide information on online safety for individuals and businesses to help protect their finances and devices from fraud and problems online. They have a website checker which shows whether a website is likely to be legitimate or not. They can be contacted via an online form.

Website: https://www.getsafeonline.org/

The Online Dating and Discovery Association (ODDA)

The ODDA is a trade association for the online dating sector. They work on behalf of the public to encourage dating sites to make their platforms safe spaces. They provide advice on dating safety online and have a facility for reporting concerns.

Website: https://theodda.org

Royal National Institute of Blind People

The RNIB supports people who have lost their sight or those who have an eye condition which could lead to sight loss. They have information about money and benefits on their website.

Telephone: 030 3123 9999 (Monday - Friday, 9am - 6pm)

Email: helpline@rnib.org.uk

Website: https://www.rnib.org.uk/

Age UK

Age UK is a charity providing companionship, advice and support for older people. Your nearest branch can be found on their website. They also have a wellbeing programme and befriending service.

Telephone: 0800 055 6112, Available between 8am - 7pm, 365 days a year

Email: general@ageuklondon.org.uk

Website: www.ageuk.org.uk

The **Silver Line Helpline,** run by Age UK, is a free, confidential, 24-hour telephone service providing friendship, information and advice to older people 7 days a week.

Telephone: 0800 470 8090

Website: https://www.thesilverline.org.uk/

Independent Age

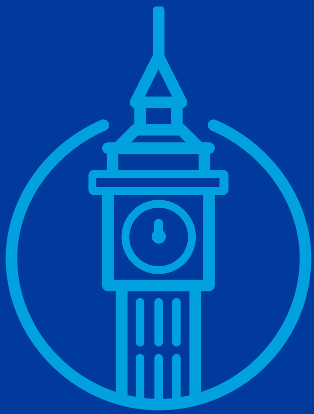
Independent Age is a national charity focused on improving the lives of older people in financial difficulty. Their helpline and advisors provide clear, free and impartial advice on issues such as care, support, money, benefits, health and mobility.

Telephone: 0800 319 6789, Monday - Friday, 8:30am - 5:30pm

Email: helpline@independentage.org

Website: https://www.independentage.org/

Their webchat services operate between Monday - Friday, 9am - 5pm



London specific support

London Victim and Witness Service

The London Victim and Witness Service (LVWS) provides tailored help if you've been affected by crime. The service is provided by Victim Support and is independent of the Police.

Telephone: 0808 168 9291

Website: https://londonvws.org.uk/contact-us/

Money A&E

Money A&E give money advice and education to disadvantaged Diverse Ethnic Communities and young people. They run workshops and have mentors and coaches. Advice appointments can be booked on their website.

Website: https://www.moneyaande.co.uk/

Brixton Advice Centre

Brixton Advice Centre provide debt advice in Lambeth and links to local organisations who can help you. Find out about managing your money, credit scores, payday loans and how to use an ombudsman.

Website: https://brixtonadvice.org.uk/debt-and-money/

Catch22

Catch22 is a not-for-profit company which aims to provide people with a purpose, a good place to live and good people around them. They help people achieve this by delivering finance, benefit and debt-related support, signposting and advocacy in London to reduce re-offending.

Website: https://www.catch-22.org.uk/find-services/finance-benefit-debt/

Telephone: 0207 733 7554

CAP Debt Help Centre London Cricklewood

The Christian's Against Poverty centre provides information to help you make the right choices about your finances including help with budgeting.

Website: https://capuk.org

Telephone: 0800 328 0006

Email: info@capuk.org

Notes

Notes