UK Fraud Protection Guide

Your complete guide to protecting yourself and your family from fraud

Produced by Silent Erase — silenterase.com — ICO Registered C1971457

Introduction

Fraud is the most common crime in the UK. Every year billions of pounds are stolen from ordinary people — and the methods used by fraudsters are becoming increasingly sophisticated. This guide will help you understand the threats, protect yourself and your family and know exactly what to do if you become a victim.

The good news is that with the right knowledge, you can significantly reduce your risk. Read this guide carefully and share it with anyone you care about — especially elderly relatives who are disproportionately targeted.

Section 1 — The 10 Most Common UK Fraud Scams Right Now

1. Romance Scams

Fraudsters create fake online profiles on dating sites and social media, spending weeks or months building a relationship before asking for money. UK victims lost over £92 million to romance fraud last year. Never send money to someone you have not met in person.

2. Investment and Crypto Fraud

Fake investment opportunities promising high returns are flooding social media. Scammers use your personal data to make approaches seem legitimate and personalised. If it sounds too good to be true, it always is.

3. HMRC Phone Scams

Fraudsters impersonate HMRC officials claiming you owe tax and face arrest if you do not pay immediately. HMRC will never call you demanding immediate payment or threatening arrest. Always hang up and call HMRC directly on 0300 200 3300.

4. Bank Transfer Fraud (APP Fraud)

You receive a call from someone claiming to be your bank saying your account has been compromised. They ask you to transfer money to a "safe account". Your real bank will never ask you to do this. Hang up and call your bank on the number on the back of your card.

5. Parcel Delivery Scams

Fake texts claiming to be from Royal Mail, DPD or Amazon saying you have a missed delivery and need to pay a small fee. Clicking the link leads to a fake payment page that steals your card details.

6. Microsoft/Tech Support Scams

A pop-up or phone call claims your computer has a virus and you need to call a number or give remote access. Microsoft will never contact you unsolicited. Never give anyone remote access to your computer.

7. Council Tax Scams

Fake emails or calls claiming you are owed a council tax refund. They ask for your bank details to process the refund. Your council will never ask for bank details this way.

8. Pension Liberation Fraud

Fraudsters offer to help you access your pension early or move it to a better scheme. This can result in massive tax penalties and loss of your entire pension. Always verify pension advice with the Financial Conduct Authority (FCA).

9. Doorstep Fraud

Strangers arrive at your door offering services such as driveway repairs, tree surgery or roofing at very low prices, then demand large sums of cash on completion. Always get multiple quotes and never pay cash upfront.

10. Data Broker Targeting

Your home address, phone number and daily routine are listed on hundreds of websites and sold to cold callers, scammers and fraudsters who use this information to make their approaches seem legitimate and personal.

Section 2 — How to Check if Your Data is Exposed

Most people have no idea how much personal information is publicly available about them online. Here is how to check:

Step 1 — Search for yourself on Google

Search for your full name and postcode. Also search your name with your phone number. See what comes up — you may be shocked.

Step 2 — Check data broker sites

Visit these sites and search for your name:
192.com
WhitePages.com
Spokeo.com
BeenVerified.com
Radaris.com

If your information appears, you have the right to request removal under UK GDPR.

Step 3 — Check if your email has been in a data breach

Visit HaveIBeenPwned.com and enter your email address. This free service will tell you if your email and password have been leaked in any known data breaches.

TIP: Silent Erase checks all of this for you automatically and sends removal requests on your behalf. Visit silenterase.com for a free scan.

Section 3 — What To Do If You Have Been Scammed

If you think you have been scammed act immediately — every minute counts.

Step 1 — Contact your bank immediately

Call the fraud number on the back of your bank card or use your banking app. Ask them to freeze your account and reverse any transactions if possible. UK banks are required to reimburse victims of authorised push payment fraud in many cases.

Step 2 — Report to Report Fraud

Call 0300 123 2040 or visit reportfraud.police.uk to report the fraud. You will receive a crime reference number which you will need for insurance claims and bank disputes.

Step 3 — Report to your phone provider

If you were contacted by phone, report the number to your provider. You can also report nuisance calls to the

Information Commissioner's Office (ICO).

Step 4 — Change your passwords

If you gave out any account details, change your passwords immediately. Use a different password for every account and consider using a password manager.

Step 5 — Tell someone you trust

Fraud can be deeply embarrassing but it happens to millions of people. Telling a trusted friend or family member can help you think clearly and take the right steps.

WARNING: Never pay money to get your money back. If someone contacts you claiming they can recover your lost funds for a fee, this is almost certainly another scam.

Section 4 — Protecting Your Elderly Relatives

People aged 65 and over are disproportionately targeted by fraudsters. Here is how to help protect them:

Have an open conversation

Talk to elderly relatives about fraud. Many are embarrassed to discuss it but knowing what to look out for is their best protection. Reassure them that fraud can happen to anyone.

Set up call blocking

BT, Sky, Virgin and most phone providers offer free call blocking services. The Telephone Preference Service (TPS) at tpsonline.org.uk can also reduce cold calls though fraudsters often ignore it.

Register with the Mail Preference Service

Visit mpsonline.org.uk to reduce unsolicited mail which can also be used for fraud.

Remove their data from broker sites

Data broker sites listing elderly relatives' home addresses are a major source of targeting by fraudsters. Use Silent Erase to monitor and remove this data automatically.

Set up a password with their bank

Most banks offer a verbal password system so elderly relatives can verify they are speaking to a real bank employee. Ask their bank to set this up.

TIP: The Silent Erase Guardian plan allows you to add up to 5 family members for monitoring — protecting elderly relatives automatically. Visit silenterase.com/pricing for details.

Section 5 — Your Rights Under UK GDPR

Under the UK General Data Protection Regulation you have powerful rights over your personal data:

Right to Erasure (Article 17)

You can request that any organisation delete your personal data. They must comply within one calendar month unless they have a legitimate reason to retain it.

Right of Access (Article 15)

You can request a copy of all personal data any organisation holds about you. This is called a Subject Access Request (SAR) and must be fulfilled within one calendar month and is free of charge.

Right to Rectification (Article 16)

If an organisation holds inaccurate data about you, you can demand they correct it immediately.

Right to Object to Marketing (Article 21)

You can object to your data being used for direct marketing at any time. This right is absolute — they cannot refuse.

How to Exercise Your Rights

You can send a formal letter to any organisation requesting they delete, correct or provide your data. Silent Erase generates these letters automatically at silenterase.com/clear-your-name.

WARNING: If an organisation refuses to comply with your GDPR rights, you can file a complaint with the Information Commissioner's Office (ICO) at ico.org.uk or call 0303 123 1113.

Section 6 — Immediate Action Checklist

Work through this checklist to protect yourself right now:

& Search for yourself on Google and note what appears
& Check your email on HaveIBeenPwned.com
& Register with the Telephone Preference Service at tpsonline.org.uk
& Enable two-factor authentication on your email and banking apps
& Use a different password for every important account
& Check data broker sites for your personal information
& Send removal requests to any sites listing your data
& Talk to elderly relatives about fraud awareness
& Save Report Fraud number in your phone: 0300 123 2040
& Save your bank fraud line in your phone
& Run a free privacy scan at silenterase.com

Section 7 — Useful Contacts

Report Fraud: 0300 123 2040 | reportfraud.police.uk
ICO (data protection): 0303 123 1113 | ico.org.uk
Financial Conduct Authority: 0800 111 6768 | fca.org.uk
Age UK fraud advice: 0800 678 1602 | ageuk.org.uk
Citizens Advice: 0800 144 8848 | citizensadvice.org.uk
Telephone Preference Service: tpsonline.org.uk
Mail Preference Service: mpsonline.org.uk
Have I Been Pwned: haveibeenpwned.com
Silent Erase: silenterase.com | admin@silenterase.com
