# Scams Information
# Briefing Paper September 2021

## Introduction

**There are many different types of scams out there and this briefing paper cannot encapsulate all of them, but it's aim is to inform you about how you can reduce your risk to getting scammed.**

The Annual Fraud Indicator estimates fraud losses to the UK at around £190 billion every year, with the private sector businesses hit hardest losing around £140 billion. The public sector may be losing more than £43 billion and individuals losing around £7 billion.

People of all ages fall victim to scams, but older people seem particularly targeted as they are more likely to live on their own, experience high levels of isolation and loneliness and health issues such as dementia that leave people vulnerable to being targeted

Age UK statistics show that 43% of older people – almost five million people aged 65 and over – believe they have been targeted by scammers. The most common loss is £500, but in many cases, people lose much more - life savings, pension pots and this can be financially and psychologically devastating.

Once people realise they have been scammed, they often feel ashamed to have been duped and so will seldom report what has happened. It is estimated that only 5% of these crimes are ever reported.

## How to spot a scam?

**Scams can be committed over the phone, through the post, on the internet or face-to-face, often on the doorstep. Below is a quick guide of how to reduce the risk of being scammed.**

**1. Do not give any personal information (name, address, bank details, email or phone number) to organisations or people before verifying their credentials.**

Question unsolicited calls, texts or emails requesting your personal or financial information (name, address, bank details, email or phone number). Contact the company directly using a known email or phone number.

**2. Make sure your computer has up-to-date anti-virus software and a firewall installed. Ensure your browser is set to the highest level of security and monitoring to prevent malware issues and computer crimes.**

Always install the latest software and app updates on all of your devices. Protect your email account with a strong, separate password and enable two-factor authentication (2FA) where possible. Installing, or enabling, antivirus software on your laptops and computers will protect them from viruses and hackers.

**3. Many frauds start with a phishing email. Remember that banks and financial institutions will not send you an email asking you to click on a link and confirm your bank details. Do not trust such emails, even if they look genuine. You can always call your bank using the phone number on a genuine piece of correspondence, website (typed directly into the address bar) or the phone book to check if you're not sure.**

Never automatically click on a link in an unexpected email or text. Email addresses and phone numbers can be spoofed, so don't use those to verify that a message or call is authentic. The best way to get in touch with a company is to use a known email or phone number.

**4. Sign-up to Verified by Visa or MasterCard Secure Code whenever you are given the option while shopping online. This involves you registering a password with your card company and adds an additional layer of security to online transactions with signed-up retailers.**

Layer up your protection. When shopping online, always check the web address to make sure you are on the correct site and sign-up to Verified by Visa or MasterCard Secure Code whenever you are given the option.

**5. You can get a copy of your credit file and check it for entries you don't recognise. Callcredit, Equifax and Experian can all provide your credit file. An identity protection service such as ProtectMyID monitors your Experian credit report and alerts you by email or SMS (text message) to potentially fraudulent activity. If it's fraud, a dedicated caseworker will help you resolve everything.**

**6. Destroy and preferably shred receipts with your card details on and post with your name and address on. Identity fraudsters don't need much information in order to be able to clone your identity.**

**7. If you receive bills, invoices or receipts for things that you haven't bought, or financial institutions you don't normally deal with or contact you about outstanding debts, take action. Your identity may have been stolen.**

**8. Be extremely wary of post, phone calls or emails offering you business deals out of the blue. If an offer seems too good to be true, it probably is. Always question it.**

Listen to your instincts and be wary of unsolicited calls, emails or online ads offering deals that sound too good to be true. Genuine banks, or other trusted organisations, won't pressure you into making a financial transaction, if something feels wrong then it's usually right to question it.

**9. If you have been a victim of fraud, be aware of *fraud recovery* fraud. This is when fraudsters pretend to be a lawyer or a law enforcement officer and tell you they can help you recover the money you've already lost.**

## On your doorstep - Be on your guard

- Put up a sign: place a sign in the window near your front door saying that uninvited callers are not welcome.
- Keep your home secure: don't let any stranger into your home. Keep your doors locked with the chain on. Ask to see callers' ID cards and call the company to see if they are genuine. To be safe, look up the company number yourself rather than trust the number on their ID card. If you feel uncomfortable or have any doubts, don't let them in. It's your home. Tell them you're not interested or that now is 'not convenient' and ask them to come back at a different time (when you can have a friend or relative with you).
- Set up a utilities password: you can set up a password with your gas and electricity providers so that you can be sure callers (such as meter readers) are genuine – only genuine callers will be aware of your password. Call your utility company to arrange this. To activate the service they might need to put you on their Priority Services Register. This gives access to extra services if you're of

pensionable age, are registered disabled, have a hearing or visual impairment, or have long-term ill health.

- Nominate a neighbour: if you have a relative or friend who lives close by, ask if they'd mind being on standby in case you get any suspicious callers on the doorstep. Before letting a stranger into your house, give your neighbour a call and ask them to pop round. If you don't know anyone nearby, contact your local Neighbourhood Watch Scheme or Safer Neighbourhood Team to find out if they can help. A genuine caller will return at a prearranged time when you're able to have someone else in your home with you.
- Consider smart security devices: smart doorbells incorporate a camera and can enable you to speak to a caller without opening the door; some can also send a message to a relative notifying them that you have a visitor. See the link in further information for more details.
- Take a photo: if you're suspicious, ask the caller if you can take their photo on your mobile phone. Then send it to a close friend or relative. If the caller is genuine, they probably won't mind.
- Call the police: if a caller is really persistent and refuses to leave, you can call 999. If you are suspicious, but not in immediate danger, call 101 – the police non-emergency number.

## On the phone - How to reduce nuisance calls

You can't stop unwanted phone calls completely, but you can reduce the risk of getting them by taking the following steps:

- Call Protect is an opt-in service, available for free to all existing and new BT home landline customers – and it's available now. To activate the service, call 0800 389 1572 from your BT landline or sign up via BT's Call Protect webpage. Once you sign up, it can take up to 24 hours for Call Protect to start working. Speak to your provider to see if they offer a similar service
- Sign up to the Telephone Preference Service (TPS).
- Invest in a caller ID service from your phone provider, and only take calls from numbers that you recognise
- Remove your details from the public phone directory.
- If you're plagued by calls from the same number, report them to the Information Commissioner's Office (ICO).
- If you receive silent/abandoned calls, report the problem to Ofcom.
- Consider buying a nuisance call blocker.

## What to do if you have been scammed?

### 1. Report it

Scams are a criminal offence under the Fraud Act and you should report them. It's estimated that 95% of scam victims don't report what's happened to them. Some scam victims feel embarrassed or guilty, but there's really no need to. The scammer is 100% to blame, not the victim.

The only way to stop scammers, and prevent them doing it again, is to report them. Contact your bank or building society to report any loss of money and also report cases to Action Fraud. Report fraud by speaking directly to specialist fraud advisers. They will also be able to give you help and advice about fraud.

Tel 0300 123 2040 - Operating hours: Mon–Fri, 8am–8pm

### 2. Talk about it

Being a victim of a scam could leave you feeling upset, anxious, guilty or scared. Talk to a close friend or relative about your feelings – they should be able to reassure you. If you're feeling low, talk to your GP, who may be able to refer you to a counsellor.

### 3. See if you can get your money back

Losing money to a scam can be extremely upsetting and leave a big hole in your pocket. Financial losses from fraud are rising and unfortunately, you can't always get your money back.

Your rights to reimbursement depend on whether the transaction was:

**Unauthorised:** something you didn't know about or approve; or
**Authorised:** something that you approved and willingly agreed to.

Banks and building societies are obliged, under the Payment Services Regulations 2009 and the Banking Conduct of Business rules, to reimburse unauthorised fraudulent losses, if they believe that you took all reasonable steps to protect your financial details.

Be warned – if a scammer talks you into giving away cash or your account details, it's very unlikely that your bank will reimburse you. Currently, there are no rules surrounding authorised payments and banks don't have to pay you back. If you believe that your bank or building society has wrongly refused to reimburse losses that were a result of an unauthorised transaction, you can take your dispute to the Financial Ombudsman Service.

Tel: 0800 023 4 567 - Operating hours: Mon–Fri, 8am–8pm; Sat, 9am–1pm

## Conclusion

There is an urgent need for stronger **political and corporate leadership**, coordination, and ambition in tackling scams. Whilst there are steps that individuals can take; the real action must come from government and companies to reduce the number of scams that people encounter.

## Glossary

**Antivirus software** - a computer program used to prevent, detect, and remove computer malware / viruses and helps protect against data and security breaches along with other threats.

**Firewall** - In computing, a firewall is a network security system that monitors and controls incoming and outgoing network traffic based on predetermined security rules. A firewall typically establishes a barrier between a trusted network and an untrusted network, such as the Internet.

**Phishing** - the fraudulent practice of sending emails purporting to be from reputable companies in order to induce individuals to reveal personal information, such as passwords and credit card numbers.

**Two-factor authentication (2FA)** - a security process in which users provide two different authentication factors to verify themselves. e.g. providing a password as the first factor and a second, different factor - usually either a security token or a biometric factor, such as a fingerprint or facial scan, or a code sent via a text message, email or phone call.

## Scam Alerts

Sign up for Which? scam alert service for all the latest scams
https://campaigns.which.co.uk/scam-alert-service

## Further Information

https://www.which.co.uk/later-life-care/home-care/scams-and-older-people
https://www.actionfraud.police.uk/a-z-of-fraud
https://www.actionfraud.police.uk/
https://www.which.co.uk/reviews/smart-video-doorbells/article/how-to-buy-the-best-smart-video-doorbell-aUBcm4n6bZbE

**National Pensioners Convention**
**Marchmont Community Centre**
**62 Marchmont Street**
**WC1N 1AB**
**London**
**www.npcuk.org**