Cyber Crime

While scams can affect anyone, evidence suggests that older people are more likely to be targeted than other age groups. There are several reasons for this. Older generations may be less tech savvy and so may fall prey to increasingly sophisticated online scams designed to get people to hand over bank details or other personal details. In addition, social isolation and a lack of confidence can also lead to older people being targeted.

Scammers are exploiting fears over coronavirus to target consumers. There's been a worrying increase in the number of scams since the coronavirus pandemic. Scammers are always coming up with new ways of tricking people, and fears over coronavirus have given them a perfect opportunity. But although the scams vary, there are some things they have in common.

Police Mutual

The way that fraudsters operate evolves quickly and there are many different types of scam in operation. Here is some of the more common types of scam and how to prevent them.

Identity fraud - is increasingly prevalent and can occur via phone, online, mail and in person and involves the fraudster trying to get hold of someone's personal information such as bank account numbers, dates of birth, address details etc.

This information is then used to either access the victim's bank accounts or else obtain credit. The consequences of being targeted in this way go much wider than the actual fraud activity itself and it can take a lot of time to deal with what has happened in terms of updating passwords, dealing with banks etc.

What to do:

- **If you live in a flat, be careful of any mail left in communal areas. Always think about who can access it and whether it can be stolen.**
- **Dispose of any mail by shredding it rather than just putting it in the bin. Fraudsters will go through people's rubbish in the hope of obtaining personal details.**
- **Sign up to the Mail Preference Service and the Telephone Preference Service to prevent marketing letters and calls.**
- **Don't disclose details such as account numbers or PINs to anyone you don't know or trust. Banks would never ask a customer to disclose their PIN over the phone or online.**
- **Check statements for suspicious transfers.**

Online fraud - has evolved quickly and takes many forms. It can be an email purporting to be from a bank or another trusted provider asking the user to input their password or account details. These emails look authentic but are operated by scammers who use the details to take money from the targeted person's bank account.

You may have received emails from someone you do not know offering to put money in your account if banking details are sent. Even if such emails do not explicitly ask for banking details they may contain attachments which, if clicked on, will infect the computer with a virus that can make personal data available to fraudsters.

Another widespread fraud is for someone to receive an email supposedly from someone they know saying they need money urgently.

Other instances of online fraud may relate to bogus websites offering services/products. The purchaser hands over their bank details for services/products that don't arrive and the fraudster now has their bank details.

What to do:

- **If you shop online or use online banking then ensure you have anti-virus software installed on your computer. It may be worth checking with your bank as it can often provide anti-virus software for free.**
- **Don't reply to any suspicious or unsolicited emails or texts as they will likely receive more. Just delete them.**
- **Never disclose PIN numbers or passwords to someone you don't know or trust. Banks would never ask for such details online.**
- **Do not respond to emails asking for money. The likelihood is that more will be sent. Just delete them.**
- **If you receive an email from someone you know asking for financial assistance then do not respond to the email but call that person instead to see if they really did send the email.**
- **Check your bank statements regularly to see if there have been any suspicious transfers.**

Pension and Investment Scams

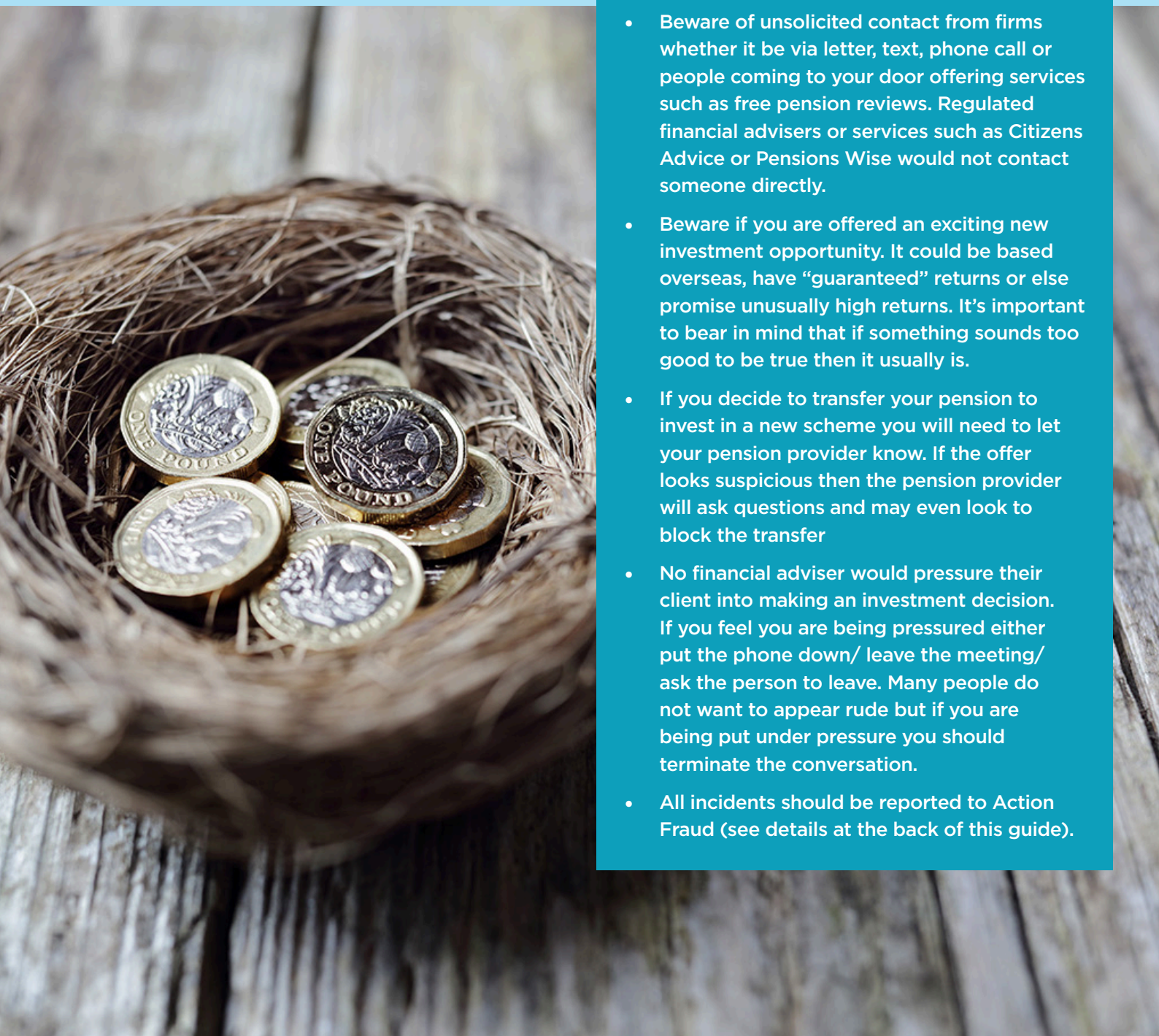
People have contributed to their pensions over many years and will often have built up a considerable sum of money. As a result, pensions have proved to be fertile ground for scammers wanting to get their hands on people's retirement nest egg. People targeted by such scams can not only find themselves losing their entire pension, but also having to pay a hefty tax bill from HMRC.

Watch out for offers of free pension reviews which come out of the blue and offers to help you move your money to a safe haven. Your money will be invested in high-risk and unregulated investments or will disappear altogether.

Pension cold calls are illegal so if you get one, just hang up – it's a sure sign that it's a scam. Ignore any offers you get via email, text or online adverts too.

Before making any changes to your pension, check that any firm you deal with appears on the FCA's Register. Then call the FCA's Consumer Helpline on 0800 111 6768 to check the firm is allowed to give pension advice.

Investment scams can operate in a very similar way to pension scams. Again, victims are contacted by someone offering an investment apparently generating high returns and often located overseas. As with pension scams the seller is likely to try and pressure someone into making a quick decision. Unlike pension scams there is unlikely to be a pension provider who will sound a warning if they feel that their customer has been targeted by a scammer.



What to do:

- Beware of unsolicited contact from firms whether it be via letter, text, phone call or people coming to your door offering services such as free pension reviews. Regulated financial advisers or services such as Citizens Advice or Pensions Wise would not contact someone directly.
- Beware if you are offered an exciting new investment opportunity. It could be based overseas, have "guaranteed" returns or else promise unusually high returns. It's important to bear in mind that if something sounds too good to be true then it usually is.
- If you decide to transfer your pension to invest in a new scheme you will need to let your pension provider know. If the offer looks suspicious then the pension provider will ask questions and may even look to block the transfer
- No financial adviser would pressure their client into making an investment decision. If you feel you are being pressured either put the phone down/ leave the meeting/ ask the person to leave. Many people do not want to appear rude but if you are being put under pressure you should terminate the conversation.
- All incidents should be reported to Action Fraud (see details at the back of this guide).

Mass marketing fraud

We have all received mail from agencies telling us we have won a prize in a draw that we don't remember entering. All you need to do to claim said prize is to send in some money and the prize will be released.

Another popular scam is to offer services or items which must be paid for upfront. However, these prizes, services or items never materialise, or else when delivered they are not of the promised quality.

These letters can look very authentic and many people decide to send in the money but their prize never arrives. What is worse is that once someone responds to one of these scams they can find themselves on so called "suckers lists" whereby other fraudsters can access their details leading to the victim being deluged with similar offers. Scammers can also start calling as well, particularly if their target has stopped responding to their letters.

These scams are particularly harrowing in terms of the effects the scammers can have on their victims. There are many instances of victims being effectively brainwashed into believing what the scammers tell them.

There have been several stories in the national media in recent years about elderly people being contacted in this way. Some have died penniless after being persuaded to hand over thousands of pounds of their money. Others have fallen out with their families. Some of these people have attempted and even taken their own lives after falling into debt and being unable to keep up with the scammer's constant demands for more cash.

What to do?

- You can check with the Trading Standards team based in the local council whether you or your friend/family member has appeared on any so-called "suckers lists."
- If you are worried your loved one may still be tempted to respond to scam mail then it is worth having a chat with them about having their mail redirected by Royal Mail.

Advance loan fee fraud

This scam involves being asked for an upfront fee in order to get accepted for a loan. The fee can be between £25 and £450 and you may be asked to pay it by bank transfer, Western Union or even iTunes vouchers. No matter how much you pay, the loan never materialises.

Warning signs to look for include being contacted by text or email out of the blue, or being put under pressure to pay the fee quickly.

What to do: You can protect yourself by checking that the firm that asks for an upfront payment is authorised by the FCA. Simply type the firm's name into the FCA's Register.

Property scams

This is a growing threat affecting the many buy-to-let landlords in the UK. These scams, known as property hijacking, involve scammers putting themselves forward as tenants so they can commit identity theft and try and sell the property from under the owner's nose.

The scammers will use fake IDs to act as tenants before changing their names by deed poll to match that of the owner. The scammer then uses fake documentation to put the property up for sale with a request for cash buyers. These potential buyers will then be pressurised into making a quick sale as this leaves less time for the scam to be discovered.

The owner is likely to find out what has happened when the buyer's solicitor attempts to register the change of ownership with the Land Registry. This is then the beginning of a long and complex process while the real owner attempts to unwind what has been done and get their property back.

What to do:

Landlords can register for a free alert service provided by the Land Registry which lets them know of any activity linked to one of their properties. This would include any attempt to change ownership details. Up to ten different properties can be monitored on one account. All you need is a valid email address and the full address/es of the properties owned. Go to https://propertyalert.landregistry.gov.uk to set up an account.

Courier fraud

Again, this type of fraud is growing rapidly. The victim is called by someone purporting to be from their bank or even a police officer to say they have noticed fraudulent activity on a bank account and need their assistance in finding the culprit.

The victim will then be asked to either disclose their PIN over the phone and the fraudster will then send a courier around to pick up the bank card to be used as evidence. Once in possession of the bank card then the fraudster can start to take money from the account.

Another popular bogus story is that the victim's bank card is about to expire and to save them the trouble of handing it in at their local branch the bank will send a courier to the person's house to collect it.

The courier despatched to pick up the items may have no idea they are involved in fraudulent activity.

What to do:

- **Just because a courier is on their way it doesn't mean they have to be let in. If in doubt don't answer the door.**
- **All instances should be reported to Action Fraud but if they are feeling in any way intimidated or frightened then they should not hesitate to call the police.**

Good cause scams

Criminals have also been targeting people with a number of scam emails asking for donations to good causes. For example, one convincing-looking email pretends to be from the government, and asks for money for the NHS. Others appear to come from an organisation that claims donations will go towards the production of hand sanitiser or protective equipment for the NHS.

What to do:

- **Don't download attachments or click on links in emails unless you're sure who sent them. Even if the email is from an organisation you know, if the email itself is unexpected or asks you to click on a link, it could be a scam. That's especially true if it asks for personal or financial information. Your bank will never ask you for personal information in an email.**
- **You can reduce the risk of being scammed by only donating to legitimate charities. You can search for a registered charity in England and Wales on the Gov.uk website charity register. If you're in Scotland, check the Scottish Charity Regulator's website. In Northern Ireland, it's the Charity Commission for Northern Ireland.**

NHS Test and Trace scams

There have been reports of scammers claiming to be from the NHS Test and Trace Service. They send a message or phone you to say you've been in contact with someone who has tested positive for coronavirus and that you need to self-isolate and take a test. They then ask you to provide your bank card details and tell you this is necessary so they can take payment for the cost of the testing kit.

Genuine tracers from the NHS Test and Trace Service may contact you by phone, email or text but they will never ask for payment for the testing kit or for your bank details.

What to do:

- **If you receive a call where they ask for payment, report it to Action Fraud. If you're in Scotland report it directly to Police Scotland by calling 101.**
- **Be careful of any links in messages you receive to the contact tracing service website. Action Fraud advises you to type the web address (http://contact-tracing.phe.gov.uk) directly into your browser rather than clicking on any link provided in the message.**

Universal Credit scams

Fraudsters have been targeting people who receive Universal Credit by claiming to offer government loans and grants linked to the benefit.

Their aim is to steal your personal or bank details.

What to do:

Remember that the government will never ask for personal or bank details over text or email so if you receive something like this, the best advice is to ignore it.

Number spoofing scams

Number spoofing is where a scammer sends a text message that looks like it's come from a genuine organisation, such as the government, HM Revenue and Customs or your bank. These scams are very hard to spot especially as the messages will sometimes appear in a chain of otherwise genuine text messages.

What to do:

Don't click on any link in a text that appears to come from a legitimate source. HMRC doesn't issue tax rebates by text, and banks don't ask for personal information this way.

Clone firm scams

This is where scammers pretend to be from an FCA-authorised firm to try and convince you they are genuine. A firm needs to be authorised by the Financial Conduct Authority to sell, promote or advise on the sale of shares or investments (including pensions) in the UK.

These fraudsters set up websites that use names similar to those of legitimate firms, and typically cold-call you to promote worthless or non-existent shares, property or investment opportunities.

What to do:

- **Protect yourself by checking the FCA register to see if the firm is authorised. Always access the FCA's Register directly from register.fca.org.uk rather than from any links sent to you by the firm itself.**
- **The FCA also recommends using the switchboard number given on the FCA Register to call the firm back rather than the one the firm gives you. If the firm claims the number on the register is out of date, contact the FCA's Consumer Helpline on 0800 111 6768.**

Cold call and doorstep scams

Not all scams are online or over the phone. Some people have reported that scammers have been going door-to-door offering 'coronavirus tests' with some posing as NHS contact tracers.

What to do:

- **Ask to see the identity badge of anyone who comes to your door and claims to be from a company or organisation.**
- **If you're not 100% comfortable, don't let them in, and don't give away financial information (such as your bank account details).**

Lookalike websites

There's been a sharp increase in the number of people visiting the websites of debt advice charities since the government introduced coronavirus measures, and scammers are taking advantage of this. They are advertising websites that offer debt advice. These sites have very similar names to the genuine services and charities. They're not illegal, but you could end up paying for debt advice that you could get for free. And you may end up sharing your personal details with a company you don't know anything about.

What to do:

If you're visiting a website to get debt advice, always check the website address to make sure you're not clicking on a 'lookalike' site by mistake.

The FCA is also warning that scammers could use any of the following tactics during the coronavirus pandemic.

The fraudsters may:

- **play on worries you have about your investments falling in value and advise you to invest or transfer your investments into investments they recommend.**
- **contact you claiming to be from a claims management company, insurance company or your credit card provider. They'll tell you they can help you make a claim for the cost of a holiday or a cancelled event and will ask you send them some money or your bank details.**
- **send you messages telling you your bank is in trouble due to the coronavirus and to transfer money to a new (bogus) bank account.**

WHO TO REPORT IT TO AND WHERE TO GET SUPPORT

Scams should be reported to:
Action Fraud
www.actionfraud.police.uk
Tel: 0300 123 2040

The Trading Standards Department at your local authority can provide support in terms of supplying call blockers or removing mail. They can also tell if you or our loved one have been included on any so called "suckers lists".

You can sign up for the **Telephone Preference Service** here:
www.tpsonline.org.uk/tps/index.html

The **Mail Preference Service** can be used to reduce the amount of mail received:
www.mpsonline.org.uk

Citizens Advice Consumer Service
offer advice about scams:
www.adviceguide.org.uk
Tel: 03444 111 445

The Pensions Advisory Service can offer guidance for those affected by pension scams:
https://www.pensionsadvisoryservice.org.uk
Tel: 0800 011 3797

Charities such as **Think Jessica** offer valuable support for elderly people and their families who have been targeted by scam mails and calls:
www.thinkjessica.com

Age UK can also offer support:
www.ageuk.org.uk
or if you are in Wales use:
Age UK Cymru
www.ageuk.org.uk/cymru

Police Mutual offer a range of wellbeing support services, for more details check out the wellbeing pages on our website: www.policemutual.co.uk

Visit policemutual.co.uk

Police Mutual

PMCC 11/20