SCAMS

Crime toolkits

DON'T BE A SCAM VICTIM!!

Scammers will use any means to separate you from your money or your personal data – they operate over the phone, through the post, on the internet or face-to-face, often on the doorstep.

They will do their best to persuade you that they, or whatever it is they are offering you, are genuine – and will usually appear to be polite, friendly, and professional. It can be easy to be taken in by them – after all, they do this for a living!

However, there are also lots of signs that might indicate that all is not what it seems. Many scams follow certain patterns, and once you know what to look for, they can be easy to spot.

Here is one of the most common scams targeted at older people, and how you can avoid falling victim to it:

DOORSTEP SCAMS

HOW DOES IT WORK?

Someone knocks at your door and claims to be a tradesman of some sort. He says he's noticed your roof needs patching up or your trees need pruning or your driveway needs fixing (or something like this). He says the work needs doing urgently and that he can do it now for a price. He'll even take you to the bank so you can withdraw the money.

There are many variations on this type of scam – sometimes the tradesman will actually do some work, though usually to a poor standard; sometimes he'll just take your money and disappear.

Sometimes the person is a salesman trying to sell you home improvements and pressing you to sign a contract on the spot.

They will do their best to persuade you that they are genuine

Sometimes he claims to be fundraising for charity and requests your bank details to set up a direct debit.

Or he might just distract you for a while on the front doorstep while his mate sneaks in through the back door and steals your purse.

DON'T BE A SCAM VICTIM!!

HOW TO DEAL WITH PEOPLE TURNING UP UNINVITED ON YOUR DOORSTEP

- Trading Standards advise all householders to NEVER BUY GOODS AND SERVICES ON THE DOORSTEP.
- Keep your front and back doors locked, even when you are at home
- Install a 'spy hole' or electronic viewer in your front door so you can see who it is before you open the door, or a door chain.
- The safest thing to do is simply not to answer the

JUST SAY NO AND ASK THEM TO LEAVE

It's not rude to ask someone to leave. Here are some things you can say to get rid of callers on your doorstep:

"I never deal with cold callers at the door, please would you leave."

"I have a neighbour who helps me, so please go and knock on their door first."

"I don't know who you are so would you please leave"

door to anyone you are not expecting.

- However, if you do answer the door, and you don't know the person, just say 'no'. Tell them you have a friend or relative who can sort out any problems. If they persist, tell them to leave or you will call the police.
- Remember – reputable traders don't need to knock on doors to get work
- Trading Standards advise that you should only use tradespeople that have been recommended to you by people you trust, or pick one from the 'Approved Tradespeople' leaflets that are distributed by local councils.

LOTTERY OR PRIZE DRAW SCAMS

HOW DOES IT WORK?

You receive a letter in the post stating that you've won a prize in a raffle, lottery or competition, and in order to receive your prize, you just have to send them your passport or bank account details so they can pay it into your bank. Oh, and they might require a small fee up front to cover the legal/tax/banking/processing charges before they can release your winnings.

DON'T BE A SCAM VICTIM!!

Don't be taken in by this. Legitimate organisations would never ask for your bank account or personal details, nor would they request an upfront fee before sending you your prize. This is a sure sign of a scam. There are other tell-tale signs to look out for, too:

SPOT THE SIGNS!!

- Does the letter contain bad spelling or grammar? If so, it's a scam. Bin it!
- There are certain letter styles that are commonly used in competition or lottery scam mail:
  - Coats of arms
  -Seals
  -Serial numbers

-Barcodes
-Watermarks
-Reproduced signatures
-Rubber stamps

- If you receive a letter with one or more of these on, and claiming you've won a prize draw or lottery, it's a scam. Bin it!
- Did you actually enter the competition or lottery in the first place? Chances are you didn't. This suggests it's a scam. Bin it!
- Have you received the letter or catalogue out of the blue, without ever asking for it or ever making contact with the company? If so, it's probably a scam. Bin it!
- Are they asking you for money? Always start from the position that any request for money is suspicious unless proven otherwise. Don't send any money!

There are also some practical steps you can take to reduce the risk that you will fall victim to a mail scam:

SIGN UP TO THE MAILING PREFERENCE SERVICE

If you are being bombarded with large amounts of mail, it's a good idea to sign up to the Mailing Preference Service (MPS). This will have the effect of stopping UK organisations that are members of the Direct Marketing Association from sending you personally-addressed mail unless you have expressly given those companies permission to do so.

However, as most scammers are unlikely to be members of the DMA, it won't stop scam mail getting through – but if you know you are registered with the MPS and ought not to be receiving any unsolicited letters or catalogues, you should be immediately suspicious of any that do arrive.

You can register online for the Mailing Preference Service at www.mpsonline.org.uk or by phoning **0845 703 4599**.
WARNING: Beware of people calling you on the phone

claiming to be from the Mailing Preference Service asking for payment to complete your registration – this is itself a scam!!

SIGN UP TO THE ROYAL MAIL OPT-OUT SERVICE

You can also opt out of Royal Mail Door to Door. This stops all unaddressed mail – post that says just 'The Occupier' or 'The Householder', for instance - being delivered to your home via Royal Mail deliveries.
If you wish to opt out, you should send your name and address to Freepost, Royal Mail Customer Services or email your name and address to optout@royalmail.com. An opt-out form will then be sent to your address, which you must complete and return.

HAVE YOUR MAIL REDIRECTED TO SOMEONE YOU TRUST

If you are always receiving large quantities of post and are not sure whether it is genuine or not, it might be worth redirecting all your mail to a relative or trusted friend, who can filter it for you and only pass on the genuine items.

REPORT SCAM MAIL TO ROYAL MAIL

If you receive written correspondence you believe to be from fraudsters, you can forward it to Royal Mail with a covering letter to: Freepost Scam Mail, PO Box 797, Exeter EX1 9UN. You can also email scam.mail@royalmail.com or call **0345 611 3413.**

EMAIL SCAMS

HOW DOES IT WORK?

Email is a favourite tool of scammers, and email scams take many forms. A common scam, called 'phishing', is where you receive an email purporting to be from your bank, which states your account has been compromised and asks you to transfer all your money to

this new, safer account they've opened for you.

There are many variations on phishing scams, too. The "bank" might invent some excuse to need your PIN number, or your online banking password.

REMEMBER: Your bank will NEVER contact you out of the blue asking for your PIN, full password or to move money to another account.

DON'T BE A SCAM VICTIM!!

If you receive an email with any of these signs, or you just don't think it looks right, just delete it. If you're not sure, ask someone you trust, like a friend or relative, or your Neighbourhood Watch coordinator.

TELEPHONE SCAMS

HOW DOES IT WORK?

Telephone calls are another popular tool of scammers. They might pretend to be your bank, and ask for your PIN number

SPOT THE SIGNS!

- The sender's email address doesn't match the website address of the organisation it says it's from. Roll your mouse pointer over the sender's name to see its true address
- The email doesn't use your name – it says something like 'Dear customer' instead
- There's a sense of urgency, asking you to act immediately
- There's a prominent website link which may look at first glance like the proper address, but has one letter missing or wrong
- There's a request for personal information- your bank will never ask for this
- There is poor grammar and spelling
- The entire text of the email is contained within an image rather than the usual text format, and the image contains an embedded hyperlink to a bogus site. Again, roll your mouse pointer over the link to reveal its true destination.

or password or tell you you've been defrauded and ask you to move your money to a safe new account.

They might even offer to send a courier to your house to pick up your bank card.

They might try to sell you investment opportunities in exotic offshore assets like diamonds or wine.

They might offer you a free review of your pension, suggesting they can convert some of it to a low-tax or tax-free lump sum.

They might say they are collecting for charity, and ask for your bank details to set up a direct debit.

Or they might claim your computer is faulty and that they can fix it, if you just tell them your password or give them access to it remotely.

All of these are scams. Just hang up the phone.

SPOT THE SIGNS!!

Any one of these 5 signs could indicate it's a scam phone call:

1.
The caller doesn't give you time to think, tries to stop you speaking to another householder or is insistent and makes you feel uncomfortable

2.
The caller asks you to transfer money to a new account for fraud reasons

3.
They phone to ask for your 4-digit PIN or online banking password. Even if they ask you to tap it into your telephone keypad rather than saying it out loud, it's still a scam

4.
They ask you to withdraw money to hand over to them for safekeeping

5.
They say you've been a victim of fraud and offer to send a courier to your home to collect your cash, PIN, payment card or cheque book.

DON'T BE A SCAM VICTIM!!

Next time you receive a phone call from someone you don't know, remember these rules to keep yourself safe from scammers:

- Never agree to anything over the phone. Just hang up if you feel at all wary of a caller.
- Don't assume a caller is genuine just because they already have some details about you, such as your name. Criminals will often already have some basic information about you.
- Remember: Your bank or building society will NEVER contact you out of the blue to ask for your PIN, full password or to move money to another account. If you receive a call from your bank requesting any of these, hang up immediately.
- Never give out any personal information over the phone, such as bank account or credit card details, unless you made the call.
- If you're not sure about a caller who claims to be from a legitimate bank or company, you can always end the call and then call the company back yourself, using a phone number from their official website or letters sent to you. Always wait five minutes before calling back though, to ensure the first caller has hung up – it takes both sides to terminate a phone call.
- Never give control of your computer remotely to a third party over the phone.
- Register your phone numbers with the Telephone Preference Service. Once you are registered, you are not supposed to receive any unsolicited sales and marketing calls from commercial organisations. Of course, scammers won't take any notice of the TPS – but if you are registered with TPS and know you are not supposed to receive any more calls, it should be obvious that any cold-callers are not legitimate.
- Mobile phone users can also

send a simple text message to opt out of unsolicited sales and marketing calls. To add your number to the UK's official 'Do Not Call' database, text 'TPS' and your email address to 85095. They will then email you to confirm your registration.

INVESTMENT SCAMS

HOW DOES IT WORK?

Investment scams can originate online, over the phone or in the post, and usually involve offers of worthless, overpriced or non-existent shares in unregulated products such as wine, diamonds or land.

Pensions scammers know that you can now access your pension in new ways, since changes to the law in 2015, and they will try to trick you into moving your pension into a new investment or converting some of it into cash at a fantastic, often tax-free, rate. They will contact you by email, phone or text and sometimes claim they are from Pension Wise or some other government-backed body. There organisations would never contact you to offer a pension review.

SPOT THE SIGNS!!

Beware of offers promising:

- A free pension or investment review
- Guaranteed returns
- Low-tax or tax-free rates, including tax-free lump sums
- Exotic sounding and/or overseas investments, such as diamonds, hotels or vineyards
- Pressure to sign up quickly.

FRAUDSTERS WILL OFTEN:

- Apply pressure to invest quickly – they might offer you a bonus or discount if you invest before a set date or say the opportunity is only available for a short period. They might even send a courier to your door to wait while you sign documents.
- Downplay the risks to your

money – they might say you will own actual assets you can sell to make back any losses or use legal jargon to suggest the investment is very safe

- Promise tempting returns that sound too good to be true, such as better interest rates than anywhere else
- Say that they're only making the offer available to you or even ask you to not tell anyone else about the opportunity

DON'T BE A SCAM VICTIM!

HOW TO PROTECT YOURSELF AGAINST INVESTMENT OR PENSION SCAMS

- Remember the golden rule: IF SOMETHING SEEMS TOO GOOD TO BE TRUE, IT PROBABLY IS!
- Reject all unsolicited contact about investments. If you're contacted out of the blue about an investment opportunity, it's very likely a scam.
- If you get cold-called, the safest thing to do is to hang up. If you get unexpected offers by email or text, it's best to simply ignore and delete them.
- Don't be rushed into making a decision – especially if they are claiming it is a time-limited offer that won't be around for much longer.
- Check to see if the investment firm or adviser is authorised on the Financial Services Register.
- Check the Financial Conduct Authority's Warning List tool to see if the investment opportunity on offer is a scam – this is a list of firms that the FCA knows is operating without permission or running scams.
- If a caller claims to be calling about a pension investment opportunity, hang up immediately. The government has made it illegal to make cold calls about pension investments, so anyone making such a call is either a fraudster, or

operating illegally. Either way, you don't want to know!

- Don't let a friend talk you into an investment – check everything yourself. People have fallen for scams because they'd been recommended by a friend. Do your homework, even if you believe yourself or your friend to be financially savvy. False confidence can lead to getting stung and with a pension, it might be years before you discover you've been scammed.

IF YOU THINK YOU'VE BEEN SCAMMED, ACT IMMEDIATELY

If you've already signed something you're now unsure about, contact your pension provider straight away. They may be able to stop a transfer that hasn't taken place yet. Then call Action Fraud on 0300 123 2040 to report it.

ROMANCE SCAMS

HOW DOES IT WORK?

Romance fraud happens when someone believes they have met their perfect match through an online dating site or app, but the other person is in fact a scammer who is using a fake profile to build the relationship. They slowly gain your trust with a view to eventually asking you for money or obtaining enough personal details to steal your identity.

This type of scam is especially insidious because the scammer is manipulating and abusing the victim's emotions. It plays on the need we all have for love and companionship and many people fall victim every year. If the scammer is successful in persuading you to lend or give them money, they will usually come back with more and more reasons for needing more.

SPOT THE SIGNS!!

People who have fallen victim to romance scams tend to report

the same pattern. If you are using online dating or friendship sites and recognise any of these signs, it may indicate you are being scammed...

Generally the scam starts with an initial contact by the scammer. The scammer may be a member of the same online dating site as you or any online forum you have joined. The scammer may also contact you on social media such as Facebook – this is why you should never accept friend requests from people you don't know.

Their profile picture is very attractive. It's common practice for scammers to use stolen photographs of beautiful people, sometimes even celebrities! Luckily, you can check whether someone's profile picture is associated with anyone else by accessing the website in Google Chrome, right-clicking on the picture and then clicking 'Search Google for image'. Google will then display any other websites that the image is on. If the person seems to have a different name on other websites, chances are they are not genuine.

The scammer will ask you a lot of questions about yourself. This is because the more information they know about you, the easier you will be to manipulate. The scammer will spin a tale about him or herself as well. Eventually you will begin speaking over the phone. This romance stage can last some time - weeks or even months.

The discussion is friendly at first, but very quickly turns romantic. They shower you with compliments and claim to be falling in love with you. Victims usually report that this shift occurs very early on in the relationship – so if it all seems to be happening too fast, it might very well be a scam.

Their story, or parts of it, change over time. If someone is making up their life story, it can be easy to forget what they've said before. If some part of their story doesn't sound quite right, or match what they said last month, that could indicate they are lying.

Their grammar and spelling is poor. Many scams originate overseas. If the scammer tells you they're from the UK, but writes as if English is not their first language, this should be a red flag.

They refuse to Skype or video call you, or meet in person. They always find an excuse as to why they can't do this.

Eventually the scammer asks you to lend them money. They use any number of reasons: they need help to pay for the flight or other transport to meet you. They are in some sort of trouble. They need money to pay for medical care, either for themselves or someone close to them. Or they have a great business or investment opportunity that could benefit both of your futures.

DON'T BE A SCAM VICTIM!!

Just because there are some mean, dishonest people out there doesn't mean you have to stop using dating sites altogether. You just have to be aware that scammers do exist, and follow some simple rules to protect yourself online:

- If you're using social media sites like Facebook, don't accept friend requests from people you don't know.
- Don't give away too many personal details about yourself online. Revealing your full name, date of birth and home address could lead to your identity being stolen.
- NEVER send or receive money or give away your bank details to someone you've only met online.
- Use reputable dating sites and keep communicating through their messaging service. Fraudsters will want you to quickly switch to text, social media or telephone so there is no evidence on the dating site of them asking you for money.

REPORTING A SCAM

If you or someone you know has been the target of a scam, and

fallen victim to it, you should report it to the police and to Action Fraud.

You should report the scam to the police by dialling 101, and to Action Fraud either through their online reporting tool https://www.actionfraud.police.uk or calling 0300 123 2040, as soon as possible. The online form takes about 20 minutes to complete.

BEEN SCAMMED? DON'T BE EMBARRASSED

- If you did fall victim to the scam, do not feel ashamed, or think that you were to blame in any way. Victims of scams are just like victims of any crime – they have been targeted by criminals and bear no culpability for the crime.
- The quicker you act, the sooner you might stop someone else becoming a victim. You might even be able to get your money back – if you sent off a cheque, for example, the police may be able to ask Royal Mail to intercept it or require your bank to put a stop on it.
- You should also tell your Neighbourhood Watch coordinator, so that they can warn others in your area that this particular type of scam is being attempted. They will not reveal to anyone else that you have been a victim of it.

ourwatch.org.uk