Advice regarding latest types of fraudsters

8 Things You Can Do To Protect Yourself Against Fraud

1. Brush up on common scams and warning signs. Read full docuent on web site.
2. Keep personal information confidential. Shred redundant statements & bills.
3. Change your passwords and PINs.
4. Keep an inventory of valuables in a safe place.
5. Watch out for unusual transactions.
6. Talk to your loved ones and inform your family about fraud.
7. Report any anomalies to bank, merchants or police.
8. Never respond to unsolicited emails, telephone calls requesting access to your computer or bank details.

Here is what my bank Nationwide advises against fraud
Think you'd spot a financial scam if you saw one? Lots of people claim they could. Yet in 2018 in the UK, £354m was lost to Authorised Push Payment scams. Could you afford to lose that kind of money – or more?
Scams have become incredibly sophisticated. And though it may surprise you, it's often the person being scammed who's responsible for the loss of their money.

Let's look at some current fraud scams

Safe account scams

You get an unexpected call from someone claiming to be from a trusted organisation such as a bank or building society or the police. They explain your money is at risk– your account's been compromised in a security breach. Then they reassure you: move your money now to a 'safe account' they've set up for you, and all will be fine. It's you who moves that money, not them. And it's money you've lost for good.

Hints and tips:
Never act on a call out of the blue and transfer money at the request of a caller. A genuine organisation would never ask you to do this.

Refund overpayment scams

You're called by a representative of a broadband or telecoms provider. You may even hold an account with them. They tell you there's an issue with your PC and will request remote access to fix it. They'll say you're due compensation for the inconvenience, and will ask you to log on to your internet bank.
Then they claim they made a mistake: they've paid you too much. What they'll actually have done is transferred money from your savings account to make it look like a refund has credited your current account. You won't know this, though, and they'll then ask you to transfer the overpayment of the 'refund' back to them.

Next thing you know, you're using your own security details to send your own money to them. And just like that, a large sum of your money is gone.

Hints and tips:

Don't allow yourself to be rushed into allowing remote access. Be sure who you are dealing with - and never log on to your internet bank account while allowing someone remote access to your device.

Investment scams

A fraudster will contact you, trying to get you involved with investments that will make you money.

They may ask you to part with some money to invest in something like wine, diamonds or alternative energy.

But the investment does not exist and you won't see any return on any money you put in.

Hints and tips:

Always visit the Financial Conduct Authority's Scamsmart website at https://www.fca.org.uk/scamsmart which offers a warning list, so you can check the risks of a potential investment. You can also search to see if the company that has contacted you is known to be operating without authorisation.

Online purchase scams

You see something (for example: a vehicle, mobile phone or concert tickets) for sale online at a price too good to be true.

Then you notice the seller would prefer you to use a different, less secure payment method than the one the selling site advises – a method that won't protect you if things go wrong.

You've been emailing the seller all along, so everything should be fine, right? But as soon as you've moved the money from your account, the emails from the seller stop. And that bargain of a car you set your heart on never turns up.

Hints and tips:

Always use a reputable website/app to buy goods. For larger purchases (for example, a car), make sure you see what you're buying before parting with any money.

Email hack scams

You have a genuine relationship with a person or company such as a builder (you may be having an extension built) or a solicitor (you may be purchasing a home).

You then receive an email telling you a payment is required; it may even tell you that the person or company's bank details have changed. You're expecting to pay them, so you think nothing of it and make the payment. You then discover that the request for payment was fraudulent. Often, this is because the person or company's email address or database has been

hacked.
If you receive a request for payment, always get in touch – using the original contact details you received – to make sure it is genuine before parting with your money.

Hints and tips:

Be vigilant – fake invoices sent over email can be very convincing. Use the original contact details you got from your supplier to contact them and check if any changes are genuine.

Rogue trader scams

You answer your door to a 'tradesperson' who tells you urgent work needs doing to your property (for example, your roof or driveway). You won't always be aware of this, but the work may not even be necessary.

The tradesperson may go on to overcharge you for work that wasn't needed. Or they may convince you to make full payment for part completed work or for materials – and never return to finish the job.
You transfer or withdraw money to pay them and then you never see them (or your money) again.

Hints and tips:

Don't feel rushed to get work done by someone knocking on your door – take your time, do your research and get quotes from several tradesmen before making any commitment.

Advance fee scams

A fraudster will contact you to ask for an upfront fee in order to receive goods, lottery winnings or a loan you have enquired about.
You make the payment – but you don't receive what you were promised.

Hints and tips:

If something sounds too good to be true, it probably is. Never part with any money without first doing some research into whether any offer you receive is genuine.

Romance scams

You meet someone new online. But can you be sure they are genuine? Maybe they're in another country – Say they need financial help to care for someone close to them, avoid persecution or to cover travel expenses to visit you.
They've earned your trust. You've developed strong feelings. What's to stop you transferring large sums of money to them? And how would you feel if you never heard from them again immediately afterwards?

Hints and tips:

Keep conversations through a reputable dating agency and never send money or receive money to someone you've only met online.

Courier scams

A fraudster will call you, pretending to be from your building society, bank or from the police. They'll claim there is an issue with your bank account,

or they'll ask for your assistance with a bank or police investigation.

As part of a fake investigation, you may be asked to take out money or to buy something. But unfortunately the fraudster only has one thing in mind – to trick you into giving them money or goods.

Hints and tips:

Do not give out your banking information (for example, you card or PIN) or take out money/buy goods for someone who claims this is necessary for an investigation. A genuine organisation would never ask you to do this.

Money mule scams

This scam involves people getting unknowingly involved with helping fraudsters move around stolen money – you effectively become a 'money mule'.

You'll see what looks like a genuine job, advertised online, on email or on social media. It'll look like a great opportunity to earn some easy money for a few hours of work every week. But any earnings you receive could be money earned from crime.

If you get involved, it could result in criminal prosecution, your account being frozen, and your information being shared with other banks as someone who cannot be trusted, which will make banking difficult for you.

Hints and tips:

A genuine company will never ask you to use your own bank account to transfer their money. Don't accept any job offers that ask you to do this. Be especially wary of job offers from people or companies overseas - it will be harder for you to find out if they are genuine.

Take Five to Stop Fraud

Nationwide supports the industry awareness campaign Take Five. They offers straight-forward and impartial advice to help everyone protect themselves against financial fraud.

Visit https://takefive-stopfraud.org.uk/

Much of the advice about came from them with some input from myself.
End of dcument