

Consumer Rights

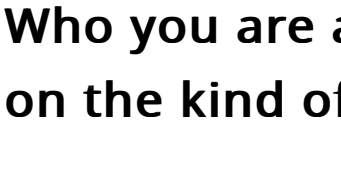
# How your personality could increase your fraud risk – and what to look out for

*Which? speaks to a cyber psychologist to understand three popular personality types and how scammers can target them*



By Adam French

29 Mar 2021



**Who you are and how you think can have a big effect on the kind of scams that are a greater risk to you.**

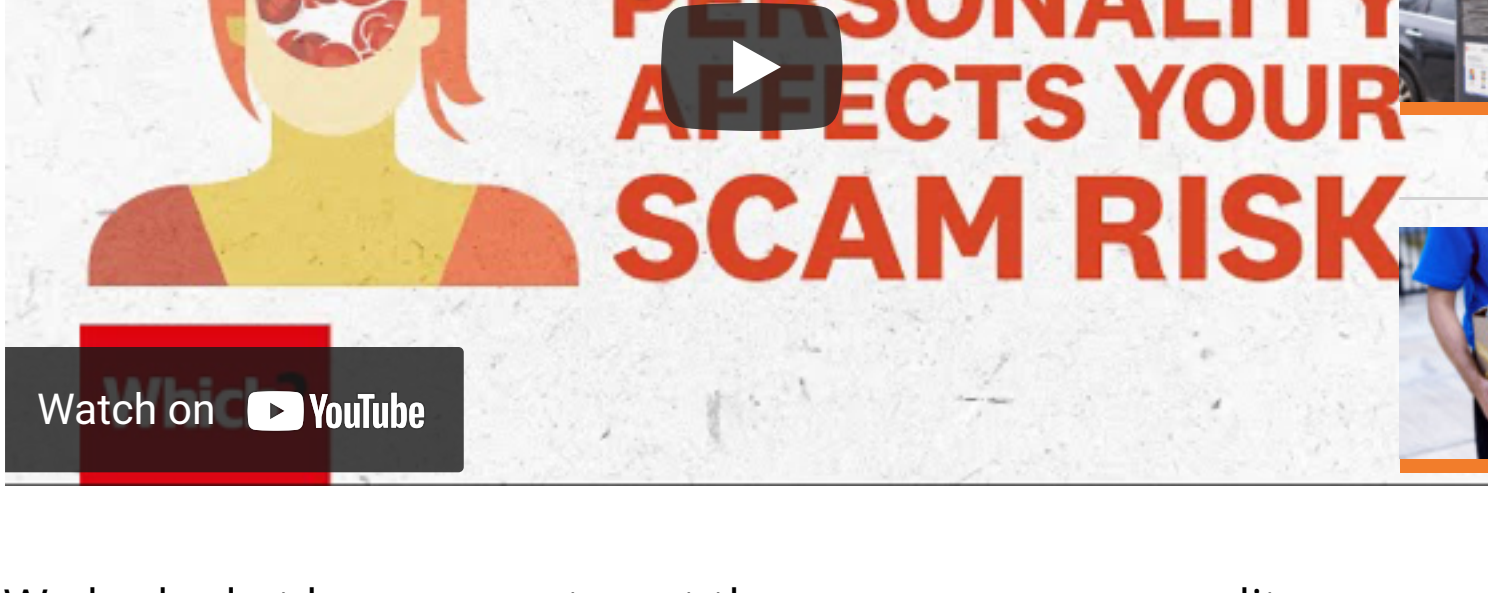
To help you understand how scammers can take advantage of who you are and how you think, we spoke to Dr Linda Kaye, a research specialist in cyberpsychology.

More on this

[A week of scams awareness](#)

[Advice to keep you safe from scams](#)

[Sign up to free Which? Scam Alerts](#)

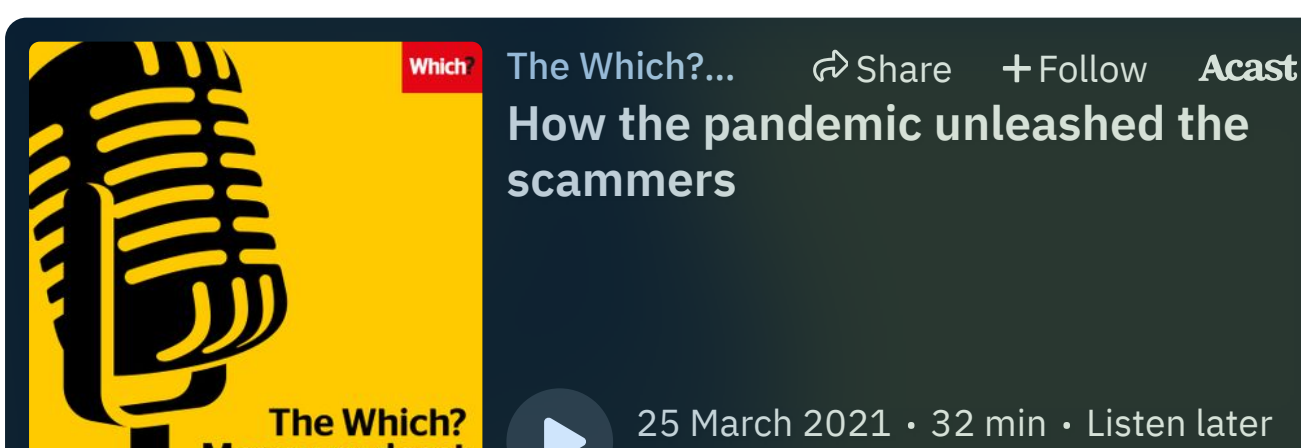


We looked at how scams target three common personality types:

- You're sociable and outgoing, usually sympathetic and happy to help
- You're inclined to worry and maybe a little temperamental
- You're quiet, reserved and prefer planning ahead rather than being spontaneous.

Here, Which? explains how your personality can determine which scams are more dangerous to you.

[Sign up to free Which? Scam Alerts and outsmart the scammers](#)



## Scams to watch out for if you're inclined to worry

Dr Kaye says: 'What we know is people who might be more fearful are maybe more likely to be caught by authority based scams. A good example of this is the HMRC scam.'

We know from our work at Which? that scams pretending to be from authority figures, such as HMRC, will often deploy threatening language to try to pressure you into acting quickly.

We've recorded scammers pretending to be from HMRC threatening potential victims with lawsuits, warrants for their arrest or demands for outstanding tax to be paid.

This is a common sign of a scam as it's designed to stop you from thinking through your actions.

### Three tips from Which? to reduce your scam risk:

- **Don't act impulsively**, especially if you receive contact out of the blue that appears to be from a figure of authority.
- **Don't follow links or share personal information**, either via email, text message or over the phone – scammers are often after your information as quickly as possible, you can always contact the organisation yourself.
- **Do your own research** to validate whether it's legitimate or not.

Listen Which? has obtained two recordings of [automated tax scam phone calls](#)



## Scams to watch out for if you're sociable and outgoing

Dr Kaye says: 'Those people who might have more social traits – so things such as agreeableness, high extroversion – may be more likely to fall for scams which are commitment-based, like romance scams.'

Dating or romance scams are when you think you've met your perfect partner online, but they aren't who they say they are. Once they have gained your trust, they ask for money for a variety of emotive reasons.

Online romance scams cost people in the UK more than £63m last year.

Watch out for someone who wants to rush things. A fraudster will usually make the first move and this will often come out of the blue.

Sometimes they will create a bogus, dreamy profile that sounds like the ideal mate you've described in your own dating profile.

They will try to play on your sympathy and strike when you are the most vulnerable.

### Three tips from Which? to reduce your scam risk:

- **If it sounds too good to be true, it probably is** Often your gut instinct will let you know something is too good to be true.
- **Beware of moving too fast** Scammers often want you to make rushed decisions before you have a chance to think things through.
- **Do your own research** to validate whether it is legitimate or not.

Read more: [how to spot a scam on a dating app or website](#)



## Scams to watch out for if you're quiet and reserved

Dr Kaye says: 'People who might be more introverted might be more likely to be vulnerable to scams such as a bitcoin scam, so ones that are characterised by things such as authority and consensus.'

'That's making someone feel that everyone else is involved in this and it's something that they should be doing because everybody else has done it.'

Bitcoin is the most famous cryptocurrency, but there are more than 1,500 cryptocurrencies, including other well-known ones such as Ethereum and Litecoin.

Cryptocurrencies are virtual peer-to-peer currencies that aren't controlled by a bank, treasury or country and only exist online – you can't get physical notes or coins from the bank.

Many legitimate businesses – such as Expedia and Microsoft – even accept cryptocurrencies as payment.

Before a new cryptocurrency is launched on an exchange, you will be able to buy cryptocurrency coins or tokens as part of an Initial Coin Offering (ICO). This is usually what's known as a pump-and-dump – when a price becomes inflated at launch, and then rapidly crashes.

If you don't understand a cryptocurrency or any other investment, avoid it. Do not hand over any money.

A scam can take many forms, it could include:

- **A fake cryptocurrency** that doesn't and won't ever exist – for example, if it's a fake Initial Coin Offering (ICO)
- **A bogus investment** that promises to put money in a legitimate cryptocurrency
- **A dangerous website link** that then downloads malware onto your computer.

### Three tips from Which? to reduce your scam risk:

- **If it sounds too good to be true, it probably is** Often your gut instinct will let you know something is too good to be true. Investment returns are many times higher than usual.
- **Beware of moving too fast** Scammers often want you to make rushed decisions before you have a chance to think things through.
- **Do your own research** to validate whether it is legitimate or not.

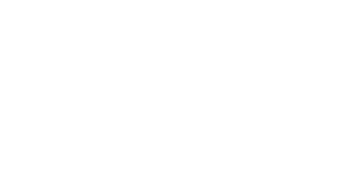
Read more: [how to spot an investment scam](#)

[Sign up to free Which? Scam Alerts and outsmart the scammers](#)

Categories: [Consumer Rights](#)

Tagged as: [Scams](#)

Did you find this useful?



Feedback