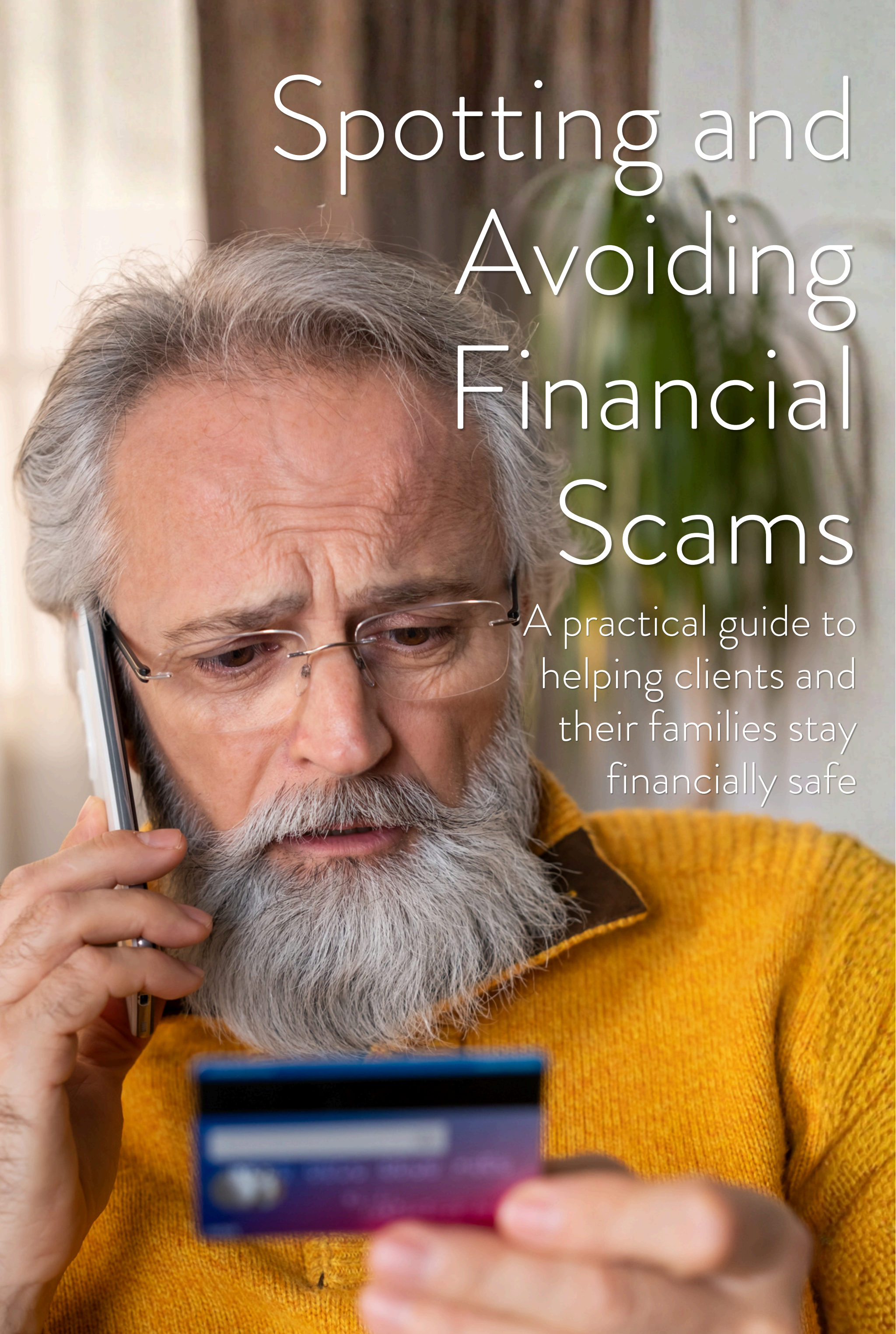

Spotting and Avoiding Financial Scams

A practical guide to helping clients and their families stay financially safe

spend time
FINANCIAL PLANNING

Fraud and scams are becoming more common and more convincing than ever.

Criminals are skilled at creating messages, calls and websites that appear genuine, often using pressure and urgency to encourage quick decisions.

Anyone can be affected by a scam, regardless of age, experience or financial knowledge.

This guide explains some of the most common warning signs, practical ways to stay safe, and what to do if something doesn't feel right.

Common Types of Scams

Investment scams
Fake investment opportunities promising high returns, low risk or exclusive access.

Pension scams
Including pension reviews, early access offers or pressure to transfer.

Banking impersonation scams
Calls or texts pretending to be your bank, HMRC, police or delivery companies for example.

Email and text phishing scams
Fake links requesting passwords, bank details or verification codes.

AI and impersonation scams
Increasingly common - cloned voices, fake WhatsApp messages and deepfake video calls

Romance scams
Relationship-building followed by requests for money.

QR code scams (Quishing)
Fraudsters replace genuine QR codes with fake ones that direct you to fraudulent payment pages or fake websites.

Payment redirection scams
Criminals intercept emails and send revised bank details, hoping you'll transfer money into the fraudster's account instead.

Common Warning Signs

Be cautious if someone:

- pressures you to act quickly
- asks you to keep something secret
- requests payment via bank transfer or cryptocurrency
- asks for passwords or security codes
- contacts you unexpectedly
- promises guaranteed returns
- discourages independent advice
- asks you to move money urgently

Even if the phone number, email address or text message appears genuine, it may have been spoofed by criminals.

Take your time
Legitimate organisations will not pressure you.

Verify independently
Use contact details from the organisation's official website or correspondence you already know to be genuine.

Pause before transferring money
Especially for large or unusual transactions.

Speak to someone you trust
Talk openly with family members about scams. Sharing experiences can help everyone recognise fraud more quickly.

Keep devices secure
e.g. strong passwords, regularly update software, use multi-factor authentication where available. Never share one-time security codes (OTP codes), even if someone claims to be from your bank. Never allow someone who contacts you unexpectedly to install software such as AnyDesk or TeamViewer or take remote control of your computer.

Be cautious on social media
Scammers often gather personal information publicly, so be careful what you post online. Be cautious of unexpected requests for charitable donations. Donate through official charity websites where possible.

Before transferring money, always ask yourself...

- Was I expecting this request?
- Have I independently verified who I'm speaking to?
- Am I being pressured to act today?
- Would I feel comfortable waiting until tomorrow?

What To Do If You Think You've Been Scammed

Suggested steps:

1. Contact your bank(s) immediately. If you have shared your debit or credit card details, ask your bank whether your cards should be cancelled and replaced.
2. Change passwords.
3. Report the scam to Action Fraud online or by phone.
4. Monitor your accounts for any suspicious activity.
5. Seek support from trusted friends or family. You can also speak to Friends Against Scams for helpful advice.

Helpful links:

- FCA Firm Checker
- Action Fraud
- Take Five to Stop Fraud
- Friends Against Scams

Remember

- Genuine organisations won't rush you
- It's always okay to hang up and call back
- Never feel embarrassed about checking
- If something feels wrong, it probably deserves another look

Our Promise To You

We will never:

- ask for your passwords
- ask for your security codes
- pressure you into making an immediate decision
- ask you to transfer money without giving you time to verify the request
- mind if you hang up and call us back using our usual number

How We Help Our Clients Stay Safe

If a client of ours ever receives a message, call or request that appears to come from us or another organisation but doesn't feel right, we encourage them to contact us directly using our usual details.

We would always rather you checked with us first.

We have robust procedures in place to protect your money if someone contacts us pretending to be you in an attempt to access your money.

We will never send you bank details by email to send money to or ask for your passwords.

Summary

Fraudsters rely on pressure, uncertainty and people acting quickly. Giving yourself time to pause and check something properly is never a bad thing and any genuine person/company should be happy to give you the time you need to check things through.

Scams can affect anyone, regardless of age, experience or financial knowledge, which is why staying aware and talking openly about fraud is so important.

By understanding the warning signs and taking a few simple precautions, you can greatly reduce the risk of becoming a victim of financial fraud.

If you're ever unsure before moving money, changing investments or responding to an unexpected request, give us a call. We'd much rather spend five minutes checking something than see one of our clients become the victim of a scam.

We're always happy to help, and let us know if you'd like to talk anything through.

We hope this has helped you feel clearer and more informed about what to look out for, how best to prevent a scam and what to do if you think you have been scammed.

If you're worried you've been targeted by a scam involving Spend Time, please contact us immediately using our usual telephone number.

hello@spendtime.co.uk spendtime.co.uk

0118 2142140

Disclaimer

Please note: The information in this guide is intended as general guidance only and should not be considered personal financial advice.

If you are unsure about a financial decision or communication, please seek advice before taking action. Let us know if you'd like to talk anything through.

20th May 2026 V1