Investment scams

New and more sophisticated investment scams are emerging all the time. Here are a few we know are prevalent at the moment, and ways in which you can protect yourself.

Clone firms

Fraudsters are using the names and details of FCA-authorised firms, including AJ Bell, to convince people they work for a legitimate company and to hand over their personal details and money.

'Clone firms' can be hard to spot. Fraudsters often impersonate current or past employees, using the company's real details – such as its address and 'firm registration number' (FRN) – or fake credentials which look very similar to the real deal. But crucially, the contact information provided will be the scammer's own.

Clone scammers typically promote worthless or fraudulent investment opportunities. They contact their victims out of the blue, or target customers who search for investment opportunities online – creating scam adverts or websites that ask for your contact details.

So how do you tell a clone firm from the real thing? Here are some tips to protect yourself:

- Remember that AJ Bell Investcentre will never contact you unsolicited with an investment opportunity.
- Check the email address. We only ever use standard email addresses, which end in e.investcentre.co.uk or @ajbell.co.uk.
- Check the FCA's Register to verify that a firm contacting you is authorised.
- Ask for the firm's FRN and contact details. If you need to call the company back, always use the genuine switchboard number given on the FCA's Register. The genuine number for AJ Bell, as listed on the Register, is 0345 408 9100.
- Check the FCA's warning list of known clone firms.
- Always remember that if an investment opportunity sounds too good to be true, it probably is.

If you're ever unsure about any message you receive from AJ Bell – or someone claiming to work for or with us – always contact us to check it's legitimate.

For more tips about keeping yourself safe, visit the FCA's ScamSmart page.

If you're ever unsure about any message you receive from AJ Bell – or someone claiming to work for or with us – always contact us to check it's legitimate.

FCA's Scamsmart website

https://www.fca.org.uk/scamsmart

Boiler room scams

A boiler room is an entity that tries to sell you fake or over-valued investments. Their aim is to take your money and convince you that you have invested in something worthwhile. When you realise your mistake, you normally won't be able to contact them or get your money back; you'll just be left holding a worthless investment.

- Boiler rooms usually 'cold call' you unexpectedly or send you unsolicited mail.
- They are trained to be very convincing and will claim to be able to help you make above average returns.
- They might even offer to pay money to you outside your pension for making an investment, which isn't allowed under financial regulations.

Remember that pension cold calling is illegal. If you receive an unsolicited call about your pension from someone you don't know, you should hang up immediately and and alert the Information Commission's Office (ICO). If you're not sure, ask if you can call them back.

Companies in the UK selling investments have to be authorised by the Financial Conduct Authority. You should always check on the FCA website that the company you are dealing with exists and is authorised.

Companies in the UK selling investments have to be authorised by the Financial Conduct Authority. You should always check on the FCA website that the company you are dealing with exists and is authorised.

Recovery fraud

If you have already been a victim of a scam, you may find yourself targeted again by fraudsters claiming they can trace lost monies or sell the worthless investment for an upfront fee, but you will receive nothing for your payment.

They may even impersonate the original fraudsters, or the liquidators or representatives of the liquidators of the fraudulent firm. The real liquidators' details can be found through Companies House.

If you suspect you have been scammed, break off all contact with the suspected firm or individual and be very wary of paying any firm or individual to recover your money. If you have lost money to a scam or suspect a firm of fraudulent behaviour, report it.

Viruses and malware

Some scammers use viruses and malware to attack computers and take them over to get access to information such as security data. They can then access your account and assets. There are simple steps you can take to protect yourself.

- Keep your anti-virus software up to date.
- Don't open suspicious looking emails or email attachments.
- Be vigilant to any unusual activity on your computer.

Find out more about how to protect yourself from scams.

AJBIC/FA-IS/20240917