

Being Scam Savvy

Scamming is big business and those involved are becoming increasingly sophisticated in the way they operate, making it even easier to fall victim despite being 'scam savvy'.

Worryingly, AI is now being used to dupe people into parting with their money with incidences of well-known and trusted personalities such as Martin Lewis, being impersonated online to persuade people to invest in fraudulent schemes.

As part of our service we are always keen to give a second opinion if you are tempted to invest in something that has not been recommended by us and would encourage you to contact your usual JFS contact for advice.

We all know there's no such thing as a guaranteed 'get-rich-quick' scheme but the scammers are good at what they do and it can be easy to get caught out. Here are our top ten Golden Rules to stay safe and be Scam-Savvy:

1. Don't be rushed into agreeing to offers or deals immediately. Insist on having time to get independent or legal advice before making a decision.
2. Don't hand over money or sign anything until you've checked their credentials. Look out for the use of things such as a PO box, mobile number or premium rate number (usually beginning 090).
3. Pay close attention to how you've been addressed if it's by email. Scams may not contain your name in full, correctly, or at all, and be suspicious if there are spelling or punctuation errors.
4. Don't just rely on glowing testimonials. Find solid, independent evidence of a company's success. You can also look them up on Companies House to see if they are registered and the Financial Conduct Authority website to check their [warning list of unauthorised and clone firms](#).
5. Never send money to anyone you don't know or trust, whether in the UK or abroad, or use methods of payment you're not comfortable with.
6. Never give banking or personal details to anyone you don't know or trust. This information is valuable so make sure you protect it.
7. Don't click on links or attachments in an unexpected email, even to unsubscribe. Delete the email and go to the organisation's own website. Don't reply to scam emails even to say no – this lets the scammer know the account is active.
8. Use strong passwords. Stringing together three random words, and including numbers and letters, can create a strong but memorable password – eg House1Car2Dog3%.
9. Scammers can hack into email accounts and impersonate the business or individual using their actual email address, mimicking their communication style to make correspondence believable. Make sure



Helen Jeffrey
Chartered Financial Planner

you check the sender is who you think it is – even if it joins an existing message thread you know to be authentic. Don't be afraid to double-check and call the company directly on a number you trust.

10. Install legitimate anti-virus and firewall software and make sure you keep it up to date.

Lots more information is available on the [Get Safe Online](#) website which is dedicated to online safety and is supported by leading organisations in banking, retail and internet security. It's a valuable resource full of easy to understand, practical information.

If you spot a scam or have been scammed, report it and get help via the [ActionFraud](#) website which also provides information on fraud prevention.

Don't be embarrassed about reporting a scam. By reporting it, you'll make it more difficult for the scammers to deceive others.

Lastly, we reiterate that if you are concerned about a financial dealing and would like a second opinion please get in touch with us.

07/2023