Investment Scams: What You Need to Know

Sophisticated criminals are taking advantage of current uncertainties and ramping up their efforts to exploit people. Even experienced investors can fall victim to scammers. Investment scam happens when you get a cold call from someone pretending to offer you the opportunity to invest in a variety of schemes or products that are either worthless or don't even exist. It's also known as share sale fraud, hedge fund fraud, land banking fraud or bond fraud.

All investment scams have one thing in common, they claim to be able to offer high levels of return for very little risk.

Phishing is still one of the most effective methods that fraudsters use to compromise accounts and gain access to company data and resources. Every day, Gmail blocks more than 100 million phishing emails! This is in addition to more than 240 million COVID related daily spam messages. Further, fraudsters may pretend to be from investment houses and target the public using WhatsApp, Facebook or SMS preying on the vulnerability of users.

The pension freedom introduced in April 2015 created an opportunity for fraudsters to target people in retirement who can access cash lump sums from their pension pots. Those in retirement may therefore be more vulnerable to investment scams.

What You Need to Do

- **Restrict Sharing Your Personal Information:** Beware of who and where you share your personal information. Once your personal information is 'out there', they can use that information in a myriad of ways from impersonating you to change your contact details, including online login details to your insurer or investment company to retrieve your funds and benefits. They can effectively take over your financial affairs.
- **Critically Analyse Your Investment Related Communications**: Look out for grammatical errors and spelling mistakes in emails or inconsistent fonts, although criminals are even starting to improve their language and syntax. Triple check the actual email address to ensure it's legitimate. This is done by clicking "respond to" and then verifying the "TO" address (but not actually sending the email). Look out for small and large deviations from the normal company email address format. The part after the "@" sign must be exactly like the web address of the business who is reaching out to you.
- **Have Strong Passwords**: Always use strong (long) passwords and if you can, use multifactor authentication. Protect your webmail such as Gmail or personal email accounts with multifactor authentication whenever it is available. Fraudsters often use weak passwords on personal email accounts to access emails from your financial institution and intercept information that they can use in 'follow-up' emails that will look as if it comes from your financial service provider.
- **Report It:** If you think it's a scam, report it to the police by contacting actionfraud.co.uk and the business you suspect is being impersonated.
- **Ignore Unsolicited Offers:** A common tactic used by criminals is to promote "investment" opportunities via social media accounts, promising large returns from a small up-front payment. Never respond to any requests to send money, or have money transferred through your account, by someone you don't know and trust.
- **Carefully Consider Any Investment Opportunities:** Don't be rushed into making an investment.
- **Use The FCA Register:** T**he Financial Conduct Authority's (FCA) register < https://register.fca.org.uk/s/>** can be used to check if the company is regulated by the FCA. If you deal with a firm (or individual) that isn't regulated, you may not be covered by the Financial Ombudsman Service (FOS) if things go wrong and you lose your money. **More information about how to invest safely < https://www.fca.org.uk/scamsmart>** .

The Sanlam Promise

Sanlam is committed to the highest standards of business integrity, ethical values and governance. Sanlam has an anti-fraud process in place to protect our investors. Our staff are trained and regularly informed of current trends in investment scam to ensure they can quickly identify any potential fraud. We also encourage our staff, clients and stakeholders to report unethical or corrupt behaviour.

- Sanlam will never pressure you into making a transaction on the spot.
- We will not contact you out of the blue using a generic email (in other words, one that is not particularly addressed to you) and then ask for personal information.

- Sanlam communication will be directed at you, greeting you by name and/or surname.
- The actual Sanlam email address will end with “@sanlam.co.uk”
- Sanlam will confirm bank account details by another means such as telephone or postal mail prior to you transferring funds for an investment.

Sanlam will never in an unsecured email:

1. State bank account for you to transfer funds – without also asking you to double check previous correspondence or confirm these details verbally with your relationship manager.
2. Ask you to carry out a test transaction online.
3. State bank account information for you to transfer funds.
4. Ask you to transfer funds into a personal account.

Remember if it sounds or looks suspicious it probably is! Please call us to let us know.

If you suspect you have been a victim of fraud:

1. Report it to the police by calling 0300 123 2040 or via their website **www.actionfraud.police.uk < https://www.actionfraud.police.uk/?utm_campaign=%7b~messageName~%7d&utm_source=emailCampaign&utm_medium=email&utm_content=%7b~mailVariationId~%7d>**
2. Report it to your bank immediately; in some cases, banks can recall payments.
3. Tell us about it by calling your Portfolio Manager/Wealth Planner or our Client Services team on 01179 752 125.