Solicitors Regulation Authority

Scams

Reviewed 25 November 2019

A scam is a type of fraud that criminals use to trick you into giving them money and personal details. Sometimes criminals will use the names of law firms, solicitors or other individuals regulated by us to make their scam seem genuine, either with or without their knowledge. Contact us [https://www.sra.org.uk/home/contact-us/] immediately if you think that a firm, solicitor or other individual regulated by us is involved.

Check our scam alerts [https://www.sra.org.uk/consumers/scam-alerts/] for details of recent and ongoing scams.

Scams can take the form of unsolicited emails, text messages, telephone calls or direct mail. They will promise you something unlikely in return for a "small fee", or try to get hold of your personal details such as

- bank account details
- your full name
- your date of birth; or
- login details to bank accounts and other sensitive online accounts.

If you have been targeted by any of the scams below, **do not give out any money or personal details**. However, if you think there's a good chance someone approaching you may be genuine, ask lots of questions—just don't give them any money or personal details up front. Most scammers will not answer your questions or will just continue to pester you for money or personal details.

Remember, if it seems too good be true, it probably is. Your money may disappear, but the thing you were promised won't appear.

Recent examples of scams and further guidance can be found at

- Action Fraud [https://www.actionfraud.police.uk/]

If you believe you have fallen victim to a scam, contact the police.

Common types of scam

A person running a scam may

- text or email you to tell **you that you can claim compensation** for "your recent accident" or **get rid of your debts** quickly;

- promise you vast sums of money in exchange for an **advance fee for helping them transfer money** out of a country (they just want your bank details);
- tell you that a "distant relative" or a foreign government official has **died and left a large inheritance** that you can claim on, if you'll just pay some administrative fees (and give them your bank details);
- try to **sell you shares or invest in high-value items** that quickly turn out to be worthless—often via an aggressive telephone call (this is commonly known as "boiler-room fraud" because of the amount of pressure they put you under);
- send you an email telling you that you need to **log onto your bank's online banking system** (for example) and link you to a login screen so they can steal your login details and your money—genuine banks will never link you to their site (this is known as "**phishing**");
- tell you that you've **won the lottery** when you haven't even bought a ticket, or been to the country where the lottery is taking place;
- promise you a fabulous new job **working from home** in return for a small fee for training materials that you will never receive, or information that is widely available for free; or
- claim to be psychic and have **news from beyond the grave** in exchange for a token fee—and your bank details.