HM Government

Financial Fraud Action UK
Working together to prevent fraud

"My Money, my info, I don't think so!"

Take Five to Stop Fraud is a national fraud awareness campaign launched to help you take back control and beat financial fraud – particularly the growing problem of bank transfer scams.

My money, my info, I don't think so!

Have you received an unexpected call, email or text asking you to provide personal or financial information or to send money? Remember to stop, take five and think before you reply.

Just because someone knows some personal details - such as your name and address or your mother's maiden name – does not mean they are genuine. They could be a fraudster. Here are some simple steps you can take to help you stay safe from financial scams. Remember:

- Banks or trusted organisations will **never** contact you asking for your PIN or full password, or to transfer money to a safe account.
- ***Never*** give out your personal or financial details unless you are **absolutely sure** you know who you are dealing with.
- ***Always*** question uninvited approaches asking for information – it could be a scam. Instead contact the company directly using a trusted email or phone number to check the request is genuine.
- Don't be tricked into giving a fraudster access to your details. ***Never*** automatically click on a link in an unexpected email or text.

Remember to always...

Trust your instincts: If something feels wrong then it is usually right to question it. Fraudsters rely on your defences being down when you're in the comfort of your own home and on people being naturally trusting.

Stay in control: Be confident - refuse unusual requests for personal or financial information. It's okay to stop the discussion if you do not feel in control of it.

And Take Five: Always stop and think before acting. Take five and say: **'My money? My info? I don't think so!'**

What to watch out for...

People aren't always who they say they are

Fraudsters use a range of tactics to target people and organisations. They often impersonate someone else and seek to exploit our naturally trusting natures.

They may pretend to be from your bank, card company, police, utility company, a government department or someone else you usually deal with and trust.

TAKE FIVE TO STOP FRAUD™

takefive-stopfraud.org.uk

HM Government

Financial Fraud Action UK
Working together to prevent fraud

If you think you have been a victim...

If you think there has been fraud on your card or bank account – or if you suspect anyone has attempted to compromise your financial details – report it immediately to your bank or financial services provider and then contact Action Fraud on 0300 123 2040 or at www.actionfraud.police.uk.

If you are in Scotland contact Police Scotland on 101.

How criminals try to contact you...

Phone: Fraudsters cold call claiming they are from a bank or another trusted organisation. They can sound convincing and often do their research to find out your basic bank and personal details first.

Text message: Fraudsters send fake texts which appear to be from your bank or another trusted organisation. They can use specialist software to place the message into an existing text conversation already on your phone from a genuine organisation.

Email: Fraudsters send scam emails which look just like a genuine one, but come from a different address and include links to a dodgy website. These may claim to be from a well-known or trusted company or organisation, like a bank, major online retailer, or technology company.

Common scams.....

Requests to move money: The fraudster contacts you pretending to be from your bank or the police and claims there's been fraud or suspicious activity on your account. They try to gain your trust and say you need to transfer your money to a 'safe account' to protect it. In reality, you are sending the money straight to the fraudster.

Invoice scams: Used to target businesses, criminals pose as a regular supplier claiming their bank account details need to change. The fraudster controls the new account and when the invoice is paid, they keep the money.

House purchase scams: a fraudster impersonates a house buyer's solicitor – typically sending an email which looks bonafide advising the house purchaser that the law firm's account details have changed. The unsuspecting house purchaser transfers funds – often running into several thousand pounds to the fraudster.

Identity scams: This involves the misuse of your personal details to commit crime. Your personal details are valuable to criminals and can be misused by them, or sold on to others. Fraudsters can also use the information to make their scam approaches appear more genuine, by quoting your details.

Courier scams: Fraudsters target their victims by calling and pretending to be from your bank or the police. They typically claim there is an issue with your bank account or ask you to assist with an ongoing bank or police investigation. It can involve making you transfer money from your account to one the fraudster controls, getting you to withdraw money from your account and handing it over, or an associate coming to your home to collect your card and PIN.

Scam mail: Scam mail victims are drawn in by a surprise win and find themselves parting with money in order to claim a prize. You should never have to pay a fee to claim a prize especially for a competition that you may never have entered.

Online shopping and auction scams: The criminal places a fake ad for a high-value item, such as a car or a holiday rental. Rather than using the payment system recommended by the website, the fraudster asks you to transfer the money straight to their bank account. It's only when the item doesn't arrive or you find the place doesn't exist that you realise it's a scam.

takefive-stopfraud.org.uk

TAKE FIVE TO STOP FRAUD™