



Scam Watch

What's your favourite prank to play? Whether it's with unsuspecting friends or the grand-kids, we've probably all pulled – and been on the receiving end of – a trick or two in our time. But what about those tricks that aren't quite as innocent – the ones that are designed to part you with your cash. Well, you'll be glad we "made you look" as we go through some of the more common pranks you should be on the look-out for.

Shoulder surfers: one of the most common ways for fraudsters to acquire your PIN is not through sophisticated techniques of card cloning, but simply by watching over your shoulder as you enter it. Always be wary of people standing behind you at cash points and when entering your PIN in a shop.

Phishing: have you won a lottery you didn't enter? Had a request from "your bank" to confirm your details? These are all phishing scams and you will end up losing money. Look out for the email originating from an unusual address, or failing to address you by name. Some can be more convincing and even look like they have been sent to you by friends. If in doubt, don't give your details out.

Hang-up, no you hang-up: imagine it – you receive a call from your bank telling you your account had been compromised and you need to act fast to save your cash! You'd do exactly as you were told right? But stop, this is a scam. Your bank would take its own steps to prevent fraud on your account, it would never require you to give out your full account number, password, PIN or hand over your card to a courier – ever. Even if you're convinced you're on the phone to your bank – never give out this information.

Payment protection insurance (PPI) refunds: you receive a text or call from someone claiming to be your bank, the Ministry of Justice, or a PPI company telling you that you're owed money from mis-sold PPI. But, you must pay an administration fee before the refund can be processed. Don't give away any money! If you have a PPI complaint, you can come to the ombudsman for free and save yourself giving your cash to claims managers unnecessarily.

Online shopping scams: many of us are beating the queues by shopping online these days – and the good news is that the majority of transactions are completed with no problem. But always be wary of a seller (or buyer) who asks you to complete transactions outside of the official payment channels like PayPal – as you may find you're not protected if the item you're buying, or the money for the goods you've sold, doesn't show up.

We hope these tips help you get ahead of the game. But if you've lost out to a fraudster, don't panic. Tell your bank what's gone wrong but if you're still not able to get things sorted out, the ombudsman may be able to help on **0300 123 9 123** or **www.financial-ombudsman.org.uk**.