Could you spot a scammer?

Keeping you safe and secure

Ulster Bank

Fraud can affect anyone – whatever your background, age or experience

And attempts can come in all shapes and sizes – over the phone, on the internet or face to face. Here are some tips on how to see if you're being targeted and how to protect yourself.

What to watch out for

There are lots of tricks that fraudsters can use, but here are some simple ways you can stop fraud before it starts.

Over the phone

Have you received calls claiming to be from your bank, or the police, saying that your account's been targeted by fraudsters? They might ask you to give them your PIN or handover your bank card via a courier. We'd never do that.

Fraudsters can even use software to 'spoof' the display on your phone, so an incoming call shows a name or number of the bank or another trusted organisation – when in fact, it may be a call from a con artist.

Remember
Never reveal your personal details, PIN or Digital/Telephone Banking log-in details. With any suspicious or unexpected call, always check by calling back using a phone number you've found yourself (eg search online) and use a different phone line (where possible). This is because the fraudster can keep the line open at their end. If a second phone line isn't available wait five minutes or try calling a friend on the line first.

Watch out for calls from someone trying to sell you investments or offering you advice on the investment of your pension fund that will lead to huge financial gain.

Remember
Even if they seem to have genuine information (like details of your previous investments), always get professional advice before you send any money.

Have you received any suspicious text messages on your mobile phone?

Remember
Always delete suspicious texts. These messages often try to trick you into giving away personal and security information. Don't phone any number or click on any links included in the text. Our text alert service gives you updates about your account, but we'll never ask you for your full PIN and password in a text or ask you to click on a link for this information.

Online

Have you received any suspicious emails?

Remember
Delete any suspicious emails – never open or reply to them. Even if the email looks to be from someone you know, if it's not the usual sort of thing they'd send, don't open it. Forward any suspicious emails that appear to be from us to **phishing@rbs.co.uk**

Have you ever been offered a free trial of a product?

Remember
Read the small print to ensure that you're not entering a contract which will result in you paying out large sums of money. Always cancel the agreement before the trial period ends if you don't want to continue to receive the goods or service.

Have you been told that you've won a prize in a lottery or competition that you haven't entered and that you need to pay some money up front or provide your bank details to claim the prize or other reward (online or over the phone)?

Remember
Never send any money or pay a fee to: claim a prize, lottery winnings, or secure an inheritance or some other financial reward.

Have you been asked to provide financial assistance to someone you've recently befriended (in person or online)? Fraudsters will often use emotional pressure and ask for money to help with medical costs or financial hardship.

Remember
Never send any money unless you are absolutely certain as to the authenticity of the person you have met.

Face to face

Have you been solicited by a tradesman to do work on your home or an individual asking to access your property?

Remember
Always check their ID and confirm their authenticity. Don't agree to anything there and then. Take time to find out about their business and shop around to make sure you're getting a good deal. Or you could check to see if any friends or family have a recommendation or contact your local Trading Standards office. Find your nearest office online at **nidirect.gov.uk/northern-ireland-trading-standards-service**

Turn over for more information

Six steps to protect yourself

1. Never give banking or personal details to anyone you don't know or trust. Your bank, or the police, will never ask you for your full PIN or password either. Use different PINs and passwords for each account, never tell anyone what they are and always protect your PIN from prying eyes when using it to confirm payments

2. Never withdraw money or make a payment or purchase as a result of a request from someone who says they're from the bank, the police or some other official body. None of these people will ever ask you to do any of these things

3. Protect yourself against identity fraud by shredding any personal documents you don't need and keeping all your statements, bills and confidential letters safe. If you move home, make sure you use the Royal Mail redirection service

4. Don't hand over money or sign anything until you've checked out the company or person. Ask around or search online to find out more information about them

5. The bank will not put a link in an email that takes you **directly** to the log on screen for Digital Banking. To confirm the authenticity of a website and make sure you aren't logging on to a fake site you should always log on using the full web address or an address sourced via a separate search. We would strongly recommend you install software that protects your computer from viruses and malware – find out more at **ulsterbank.co.uk/rapport**

6. Avoid using the 'auto complete' option when completing forms online as the software is easy for thieves to access. It's always better to fill forms out manually

Who to speak to if you're worried

If you think you've been approached by fraudsters, or just have more questions, there are lots of people that can help. Don't be embarrassed, just get in touch.

- Speak to a member of staff in branch or on the phone
- Talk to a trusted family member or friend
- Get independent advice – the Citizens Advice Bureau (CAB) – visit **citizensadvice.co.uk**
- You can also call the Financial Conduct Authority Consumer Helpline on **0800 111 6768**
- Report any potential fraud to the police and to Action Fraud by calling **0300 123 2040**, or by visiting **actionfraud.org.uk**

Keep updated with tips and guidance

Visit **ulsterbank.co.uk/securitycentre** regularly to keep you updated on any new scams and to stay ahead of the fraudsters. There's lots of helpful guidance, and answers to common questions.

If you would like this information in Braille, large print or audio format please contact us on **0800 015 4422**

ULST7932NI Nov 2015