# Fraud And Security

Keep your money safe with our essential fraud prevention tips

## Stay alert, stay safe

We tend to think of fraud as something that happens to other people. In reality, anyone can be a target, so it's important to stay alert.

There are lots of things we do to protect you, but learning about common scams and the tactics criminals use can help you spot when something's not right.

Remember, we'll never ask you to:

- tell us your card's 4-digit PIN
- share your or Secure Key code
- transfer money anywhere, including to a 'safe' account
- send us your card, cheque book or cash

## Stop, challenge, protect

We've been hard at work developing tools and techniques that make it safer, but it's not enough. We need your help. If we all work together and follow a few simple steps, we can be better protected and keep your money safe – and that's good for everyone.

If you're contacted out of the blue by phone, email or text:

- **stop** – If someone contacts you unexpectedly and claims to be from a trusted organization, be suspicious. Take a moment to stop and think before sharing personal or financial information
- **challenge** – Could it be fake? It's ok to reject, refuse or ignore any requests or simply say no. Only fraudsters will put you under pressure to act urgently.

- protect – Don’t click on unfamiliar links or call numbers from texts or emails. Instead, check they’re genuine by going to the official website. Fraudsters may appear genuine, but their actions and requests are not.

## How can I protect myself?

• Always question uninvited approaches Instead, contact the company directly using an email or phone number that you can check is genuine.

• Don’t share personal information Never reveal your password or share your card details over email. Be careful with the level of detail shared on social media sites and check your privacy settings.

• Never mislead the bank about the purpose of a payment. Criminals will often try to persuade you to tell the bank that the payment is for something different to what they have told you. They may suggest it will go through smoother or the bank may stop the payment otherwise. This is a clear

sign of fraud.

• Stay safe online Always update your computer, tablet and smartphone operating systems as soon as they become available and install anti-virus software.

• Shop safe online If you’re buying something online and you don’t know the seller, never pay by bank transfer. Always use a credit card, debit card or PayPal – or a payment option that offers some protection against fraud.

• Register for Voice ID is making telephone banking safer than ever. It makes it easier to access your account through telephone banking and there’s no need to use your security number.

• Update your passwords Try to change your passwords at least twice a year. Don’t use a password that can be easily guessed and make sure that your Online Banking password isn’t the same one you use for other websites.

• Check bank statements regularly If there are any transactions that you don’t recognize, always contact us.

• Shred important documents Shred any paperwork that reveals personal information, such as bank statements, card details and other sensitive data.

• Check your credit report If someone has used your name to take out a loan or credit card, it may not show on your statements. Check your credit report at least once a year for any unusual activity.

## If you think you’ve been targeted

Call us straight away on +44 7537130272, or you can also forward any suspicious emails or texts to us at support@finfluxnow.com.