Scam awareness

Santander

Common types of scams and top tips

Invoice

- **Never** set up new payment details, or amend existing ones, without checking the request directly with the person or company you're paying. Make sure you use an existing or publicly available contact number for them and not the one in the correspondence.

Email/phishing and text/smishing

- **Don't** ever assume a communication is genuine.
- Phone numbers, email addresses and names **can be spoofed** to look real.
- **Never** click on a link, scan a QR code or download an app that allows remote access to your device.

Impersonation

- **Never** transfer or take money out of your account if you're asked to – even by your bank.
- **Never** return an overpayment or payment you've received in error before checking that it isn't part of a scam.
- **Anyone** can be impersonated, the police, your bank, even friends and family. Always check who you're speaking to.

Purchase

- If buying from a reputable site like eBay, Airbnb or Autotrader, stick to their payment advice. **Never** communicate outside the site.
- **Take time** to check the seller is genuine. If you're buying a large item such as a car, make sure you see it in person before making any payment.

Investments

- **Research** the company in full using the FCA ScamSmart website, so you know who you're dealing with.
- **Don't** feel rushed or pressured to part with your money.

Friendship and romance

- Pictures can be edited, and fake profiles are common. **Check** if the person you're talking to is who they say they are. You can check this by doing a reverse image search on any web browser.
- **Don't** lend someone money. No matter how urgent their reason. Talk it through first with someone you trust before doing anything.

Protect your devices

- **Enable** automatic updates on your device. Regularly review your privacy settings.
- **Use** locks, PINs or biometric authentication to prevent criminal access. Enable auto-lock features.
- Activate Find My Phone features to **find, lock and erase your device remotely** should you lose it.
- **Enable** multi-factor authentication (MFA) this can be a passcode or biometrics.

Protect your information

- **Protect** your privacy and **don't reveal too much information online**, especially on social networks.
- It's not just what you share online. Be careful with what you're **sharing with strangers** in person, or over the phone.
- Before you click on a link in a social media post or on a search engine, play Sherlock. **Check** the URL is secure. Go direct to the website you wanted.

Useful websites and contact information

- If you're worried, or think you've been a victim of a scam, call us on **0330 9 123 123** or **0800 313 4321** (freephone). You can also report it to Action Fraud, by calling **0300 123 2040**.
- **takefive-stopfraud.org.uk**
- **moneyhelper.org.uk**
- **actionfraud.police.uk**
- **citizensadvice.org.uk**
- **santander.co.uk**

Santander can provide literature in alternative formats. The formats are: large print, braille and audio CD. If you'd like to register to receive correspondence in an alternative format please visit **santander.co.uk/alternativeformats**. For more information, ask us in branch or give us a call. If you are deaf, have hearing loss or speech loss, please use Relay UK at **relayuk.bt.com**. This is a free service that can help you communicate over the phone. If you're using British Sign Language (BSL) and would like to use video relay, you can learn more at **santander.co.uk** by searching 'accessibility'.

MORTMC0789 FEB 25 IPG CD T