Customer Advice

Scams

Emails from unknown persons or organisations should be treated with extreme caution and deleted, unsolicited phone calls that request financial help must be disconnected immediately. Pressure to act quickly or extravagant success stories of others are tell-tale signs of a suspected scam. **Never** add your card details into unsolicited links or pop-up advertisements as these are frequently a scam.

Mystery Contact

Trusted financial organisations will never contact you asking for your PIN or passwords. Remember it is okay and not impolite to question or say no to someone who is asking odd questions. If it is too good to be true then it probably is a scam.

Password & PINS

Do not share or write down your PIN or passwords for anyone – including friends and family. PIN and passwords must be unique, hard to guess and changed regularly. If you lose your card, block it immediately via your BoosterApp.

Basic online security

Do's & Don'ts:

- do not access your BoosterApp on public computers
- regular install updates on your device
- change your passwords regularly
- keep passwords & PIN number safe. Do not share with anyone or make them easy to guess

Suspicious Activity

Occasionally you may find activity on your card that appears unusual or a transaction you do not recognise. If this occurs and it concerns you must then first temporarily block your card via your Booster App.

Next, please call our Contact Centre to notify Booster of the unusual activity on your card.

When noticing suspicious activity consider if this could be related to a genuine transaction you participated in. Transactions made online often use a trading name that is different from the online website you shopped with. A quick search online can provide clearer information about the online shop.

Disputing Transactions

You are able to complete a Transaction Dispute Form if you still are concerned. This form can also be found on our website. Contact centre staff will ask further questions to clarify and provide the best information and solution for you. A **Disputed Transaction Form** can if required be emailed to you to complete and return to us. A team will then investigate and keep you informed of progress and outcome of the investigation.

Common Scams

Inheritance Scams

Victims are contacted normally via email and advised they have inherited a large sum of money from a previously unheard-of relative overseas. This story usually involves a tale about how the money is unfortunately held up by unpaid taxes or other unpaid fees and the victim must now pay to release the money. They often provide 'authentic' documentation as proof of the inheritance and may ask for money to release the inheritance be sent to them via money transfer agents.

If you have never met the person that has died and did not know they existed before being contacted – do not send any money.

Invoice Scams

Business email account or business system hack by scammers normally tell customers of a change in bank account details or send another email advising a different account number within the body of the email than that provided in the invoice. As this email comes from one similar to the business and usually reflects expected payments, scammers can often be successful. Money lost in this manner often cannot be recovered.

If you are ever suspicious of an email, call the company and confirm the account number and payment request before you make a payment.

Lottery Scams

Victims are informed they have won a large sum of money in a lottery by scammers and then they are asked to send money to release the winnings. Once money is sent to the scammer, communication with the victim will cease.

If you did not know about the lottery or did not buy a ticket - do not send any money.

Online Job Scams

Online job scams involve an employer asking the victim to accept money into their bank account and then have the victim forward the money on elsewhere. The victim receives a commission but the forwarded money is stolen from other people. Accepting and then transferring stolen money, could lead the victim to be held liable and investigated by police.

Do not accept or forward funds on behalf of another person met through a job ad.

Online Relationship Scams

Scammers approach victims through chat rooms, social media, dating websites and unsolicited emails. Once they have developed a relationship and gained trust with their intended victim either as a friend or romantic interest they use various stories to request financial assistance or access to account details. Once successful, requests for financial help keep coming.

Use extreme caution if you are asked to send money to someone you have met online and avoid communicating online if you have not met someone in person.

Phishing Scams

Similar to phone scams, except in this instance scammers will email or text victims to encourage you into providing sensitive information often with an offer to click on a link.

Never click on the link or reply to unsolicited or untrustworthy texts or emails purporting to be from a reputable organisation.

Phone Scams

Scammers phone call victims to tell a story of woe or peril typically that will encourage sympathy and lull you into providing personal and financial information or access to your computer.

Phone calls you do not expect from persons you do not know, should be treated with extreme caution and disconnected.